UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO DE GESTÃO E ECONOMIA
ESPECIALIZAÇÃO EM MBA EM GESTÃO EMPRESARIAL

# VULNERABILIDADE DAS INFORMAÇÕES EMPRESARIAIS ATRAVÉS DO USO DE DISPOSITIVOS MÓVEIS

MONOGRAFIA DE ESPECIALIZAÇÃO

**CURITIBA**
**2015**

FRANCIANE GHAZAL

# VULNERABILIDADE DAS INFORMAÇÕES EMPRESARIAIS ATRAVÉS DO USO DE DISPOSITIVOS MÓVEIS

Trabalho de Conclusão de Curso de Especialização apresentado como requisito parcial para a obtenção do título de Especialista em MBA em Gestão Empresarial.

Orientador: Prof. Dr. Francis Kanashiro Meneghetti

**CURITIBA**

**2015**

**TERMO DE APROVAÇÃO**

**VULNERABILIDADE DAS INFORMAÇÕES EMPRESARIAIS ATRAVÉS DO USO DE DISPOSITIVOS MÓVEIS**

Esta monografia foi apresentada no dia 22 de outubro de 2015, como requisito parcial para a obtenção do título de Especialista em Engenharia da Produção – Universidade Tecnológica Federal do Paraná. O candidato apresentou o trabalho para a Banca Examinadora composta pelos professores abaixo assinados. Após a deliberação, a Banca Examinadora considerou o trabalho _____.

_____
Profª. Dr. Francis Kanashiro Meneghetti
Orientadora

_____
Profª. Drª. Áurea Cristina Magalhães Niada
Banca

_____
Profª. Dr. Paulo Daniel Batista de Sousa
Banca

Visto da coordenação:

_____
Prof. Dr. Paulo Daniel Batista de Sousa

GHAZAL, Franciane. Título do trabalho. Vulnerabilidade das Informações Empresariais Através do Uso de Dispositivos Móveis 2015. 18f. Monografia. (Especialização em MBA em Gestão Empresarial) – Programa de Pós-Graduação em Administração-PPGA, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

## RESUMO

Objetivo: Descrever estratégias de segurança da informação e as vulnerabilidades originadas do uso de dispositivos móveis na organização analisada. Métodos: Estudo de caso através de pesquisa qualitativa com área técnica, de forma descritiva e Ex-Post-Facto Seccional de uma organização com 502 usuários ativos e com banco de dados de 2,3 milhões de clientes. Resultados: A organização apresenta uma política de segurança da informação estruturada e adotou ferramentas com para evitar vulnerabilidades. Conclusão: A pesquisa demonstrou a vulnerabilidade das informações empresariais através de um ataque *Spear Phishing.*
**Palavras-chave:** Dispositivos Móveis; Segurança da Informação; Política de Segurança; Vulnerabilidade.

GHAZAL, Franciane. Título do trabalho. Vulnerabilidade das Informações Empresariais Através do Uso de Dispositivos Móveis 2015. 18f. Monografia. (Especialização em MBA em Gestão Empresarial) – Programa de Pós-Graduação em Administração-PPGA, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

## ABSTRACT

Objective: Describe security strategies of information and the vulnerabilities arising from the use of mobile devices in the analyzed organization. Methods: Case study through qualitative research with technical area, descriptively and Ex-Post Facto-Sectional of an organization with 502 active members and 2.3 million customers database. Results: The organization has a security policy of structured information and adopted tools to prevent vulnerabilities. Conclusion: Research has shown the vulnerability of enterprise information through Spear Phishing attack.
**Keywords:** Mobile Devices; Information security; Security Policy; Vulnerability.

**SUMÁRIO**

# 1 INTRODUÇÃO

Com a utilização de dispositivos móveis em ambientes corporativos, como celulares, notebooks e tablets, extensivas informações circulam diariamente pela internet, e por consequência, a segurança da informação e a confiabilidade são apenas utopias para organizações que não desenvolvem a segurança da informação, tornando-se suscetíveis a ameaças que podem comprometer a confidencialidade das informações empresarias. As organizações tornaram-se alvos preferenciais de ataques por deterem informações sigilosas e de alto valor no mercado digital, como exemplo, cita-se o banco de dados, uma vez que este retém informações confidenciais e importantes sobre clientes, de tal forma que, o vazamento de informações empresariais torna-se uma das maiores ameaças à segurança da informação corporativa.

# 2 FUNDAMENTAÇÃO TEÓRICA

## 2.1 Segurança de dispositivos móveis

Com o objetivo de contribuir confiabilidade das informações empresariais, é de responsabilidade das organizações aplicarem e realizarem o gerenciamento da política de segurança da informação (PSTI), sendo que esta representa as normas e os procedimentos que determinam as responsabilidades relativas à segurança dentro da organização. Segundo a Norma NBR ISO/IEC 27002:2013 Tecnologia da informação – Código de prática para a gestão da segurança da informação, "convém que perímetros de segurança sejam definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis" (ABNT-27002:2013, p. 38). No que se refere a circulação de dados pela rede mundial de computadores, Cláudia Szafir-Goldstein e Cesar Alexandre de Souza (2003), autores do artigo cientifico sobre a tecnologia da informação aplicada à gestão empresarial, estabelecem que a internet e os dispositivos móveis com acesso a dados permitem a concessão de informações em qualquer momento ou local, por conseguinte, dispositivos móveis conectados à rede podem conceder informações em qualquer local para parceiros, concorrentes, clientes e consumidores. Rainer e Cegielski (2012) sustentam que para proteger as informações empresariais, é necessário que haja a implementação de controles ou mecanismos de defesa que visam proteger todos os componentes de um sistema de informação. Para McCarthy (2012), o crime cibernético, também denominado virtual, tornou-se uma indústria altamente lucrativa e tem como alvo empresas que manipulam dados que podem ser úteis para esses fins. Assim sendo, cabe as organizações prepararem-se para cenários que representem alto risco aos seus negócios e minimizar possíveis ataques que podem ser originados por usuários internos e externos à organização e que tenham como objetivo transmitir dados estratégicos por meio de dispositivos móveis. Turban e Volonino (2011) definem que "as empresas precisam investir em segurança de TI para proteger seus dados e outros ativos, sua capacidade operacional e seus rendimentos líquidos" (TURBAN; VOLONINO, 2011, p. 121). Desta maneira, se as vulnerabilidades não forem detectadas e protegidas, tornam-se potenciais riscos para ataques, sendo que, mesmo que se tenham tecnologias de defesas, incidentes de tecnologia da informação podem ocorrer principalmente porque os usuários não seguem práticas e procedimentos de segurança adotados pela empresa. Diante disso, pode-se afirmar que o estabelecimento de uma política de segurança da informação define as diretrizes e normas a

serem seguidas pelos usuários da organização, inclusive com penalidades em caso de violações ou tentativas de burla, visto que, para FONTES (2012), “a construção de regulamentos de segurança da informação define padrões e procedimentos que devem ser seguidos por todos. (FONTES, 2012, p. 90).

Contudo, este artigo visa contribuir para a produção do conhecimento sobre o tema da vulnerabilidade das informações empresariais através do uso de dispositivos móveis, e tem como objetivo explorar as políticas e estratégias de segurança da informação na organização analisada, tal como as vulnerabilidades originadas através do uso de dispositivos móveis. Portanto, trata-se de um estudo de caso em uma entidade associativa de direito privado, sem fins lucrativos, localizada no estado do Paraná, através de uma pesquisa qualitativa com área técnica, esta denominada tecnologia da informação e da comunicação.

## 3 MÉTODOS

Trata-se de uma pesquisa de abordagem qualitativa com área técnica, com análise da unidade denominada tecnologia da informação e da comunicação de uma organização associativa de direito privado, sem fins lucrativos, instituída sob forma de serviço social autônomo, com sede e foro no Paraná, responsável por 502 usuários ativos e um banco de dados de 2,3 milhões de clientes. O instrumento de coleta de dados utilizado para a pesquisa foi um questionário aplicado aos 5 colaboradores, denominados analistas de negócios, que exercem suas funções dentro da unidade na organização mencionada, portanto, foi realizada a análise dos questionários, contribuindo para o levantamento de informações e descrição dos resultados, sendo que a interpretação dos dados foi realizada através da análise de conteúdo.

## 4 RESULTADOS

A amostra do estudo conteve cinco colaboradores da área de tecnologia da informação e da comunicação, estes denominados consultores, sendo que dois consultores possuem como formação técnica a profissão de administradores, subsequente de dois consultores engenheiros da computação e um consultor com formação técnica em sistemas de informação. A cerca do tempo de experiência na área, foi constatado que um consultor possui experiência inferior a dez anos e os demais possuem de quatorze a dezoito anos de experiência na área, sendo que, em relação ao tempo de experiência na empresa, foi exposto que dois consultores possuem cinco ou menos tempo de experiência, concluindo-se que os demais possuem de sete a dezesseis anos de contratação.

O estudo relatou que 502 usuários ativos acessam diariamente os sistemas da organização e os acessos são disponibilizados conforme concessão realizada pela área de tecnologia da informação e da comunicação através da avaliação do perfil do usuário, visando determinar quais serão os ativos a serem utilizados pelo mesmo durante a atuação profissional. Durante a abordagem qualitativa, todos os entrevistados souberam descrever a política de segurança da informação (PSTI) da organização, dessa forma, ficou constatado que a PSTI refere-se a um documento de conjunto de normas, obrigações, métodos e procedimentos, a fim de resguardar a organização de possíveis ameaças, essas normalmente destinadas aos softwares e hardwares da mesma, devido ao armazenamento de informações confidenciais e que podem representar elevado valor de mercado. Contudo, foi verificado que a PSTI possui um padrão de revisão continuo, a fim de garantir a segurança e conhecimento acumulado, como métodos e estratégias desenvolvidas durante a história da organização, sendo que em relação ao objetivo da PSTI, conclui-se unanimemente que a mesma deve estabelecer os princípios e parâmetros a serem seguidos pelos usuários da organização, garantindo a segurança da informação e a confiabilidade das informações, além de garantir a integridade dos ativos de segurança da informação e da comunicação (ATICs). Em relação a aplicação da PSTI, foi evidenciado que a mesma é empregada a todos os funcionários, estagiários, prestadores de serviços, terceirizados, conveniados, credenciados, fornecedores, clientes, menores aprendizes, ou quaisquer outros indivíduos ou entidades que venham a ter acesso e ou utilizar, direta ou indiretamente, as informações e os ativos de segurança da informação.

No que se refere aos procedimentos adotados pela organização para manter os sigilos das informações, foi declarado que a organização dispõe de uma norma que visa garantir que

quaisquer informações geradas, acessadas, manuseadas, armazenadas ou descartadas durante o exercício das atividades pelo indivíduo responsável, bem como todos os ativos de tecnologia da informação, são de propriedade e direito exclusivo da organização, dessa forma, devem ser aplicado somente para fins profissionais na organização, à vista disso, é proibido qualquer divulgação ou cópia sem a prévia autorização por escrito do Comitê de Segurança da Informação e da Comunicação (CSIC), entretanto, durante a abordagem qualitativa, um dos colaboradores afirmou que esse procedimento existe mas não pode-se confirmar o cumprimento rigoroso dessa normativa, uma vez que não existem meios ativos para verificação dos fatos. Em referência ao uso indevido da propriedade intelectual da organização, foi referido que a mesma desautoriza o uso das marcas, identidade visual ou qualquer outro sinal distintivo da organização, sem autorização formal, inclusive em meios acadêmicos. Entretanto, dois entrevistados afirmaram que não existe um controle especifico em relação ao uso indevido da propriedade intelectual da organização, ou seja, no quesito de sigilo de informações e uso indevido da propriedade intelectual, foi evidenciado que não existe um rígido controle em relação ao uso desses ativos. No tocante ao uso de ativos pessoais de tecnologia da informação, foi declarado que a utilização interna é permitida desde que haja uma solicitação formal, autorizada pelo gerente do usuário, e fundamentada pelo mesmo. Segundo os entrevistados, esse processo ocorre de forma fidedigna em caso de uso de notebooks particulares, entretanto, foi afirmado unanimemente que o uso de dispositivos móveis, como celulares e tablets, não exigem autorização formal, mas, neste caso, os dispositivos não autorizados não utilizam a rede corporativa, e sim uma rede própria denominada “visitante”.

Sobre a política da organização quanto a softwares de comunicação instantânea, foi evidenciado que são permitidos softwares homologados pela UTIC da organização e que atualmente a mesma dispõe de dois, sendo um denominado “Easychat”, de uso exclusivo do callcenter (central de atendimento que realiza a interface com o cliente), e o outro denominado Skype for Business, disponível para colaboradores efetivos, estagiários e terceirizados. No que concerne a política da organização quanto a áudios, vídeos e fotos, foi afirmado por todos os entrevistados que é proibido atos de gravação, vídeo ou foto dentro das dependências da organização sem a devida autorização formal. Todavia, durante a abordagem qualitativa, foi declarado por dois dos entrevistados o fato de que não existe um controle rígido quanto a divulgação desse tipo de material, apesar da organização possuir uma ferramenta que realiza o rastreio à menção ao nome da organização, sendo que, foi proferido

que esse controle é de responsabilidade da área denominada Unidade de Marketing e Comunicação.

Quanto a política da organização sobre o compartilhamento de informações com terceiros ou prestadores de serviço, foi mencionado que esse fator deve decorrer dos termos de confiabilidade e de cláusulas contratuais, uma vez que estes preveem que é proibido o compartilhamento desde que não haja autorização formal e por escrito, entretanto, um dos entrevistados não soube responder essa questão. Foi questionado sobre a possibilidade de o usuário realizar instalações de softwares nos ativos de tecnologia da organização, e foi constatado que não é possível, uma vez que devido a apontamentos de auditorias, foi estabelecido que quando necessário, deve-se entrar em contato com a UTIC, através de chamados via service desk, para que a mesma realize a instalação, desde que o uso seja exclusivamente profissional.

Sobre a existência de termo compromisso no qual o usuário compromete-se em cumprir as regras e instruções impostas na política de segurança da informação, ficou esclarecido que no momento da contratação o mesmo se compromete a respeitar e cumprir a PSTI, sendo esse processo realizado pelo setor denominado recursos humanos, entretanto, um dos entrevistados não soube responder sobre esse questionamento.

No tocante ao monitoramento de acessos a informações originadas dentro da rede da mesma, foi proferido que existe um monitoramento eficaz, uma vez que a unidade de tecnologia da informação e da comunicação utiliza softwares que realizam o controle, identificando usuários, dados de navegação e recebendo alertas de incidentes. Durante as entrevistas, também foi questionado sobre a existência de capacitações que evidenciem a importância da segurança da informação, e foi informado que a organização possui um Programa Anual de Conscientização em Segurança da Informação para capacitação e disseminação da cultura de segurança da informação junto aos seus colaboradores, este realizado pela Universidade Corporativa da mesma, entretanto, um entrevistado afirmou que no ano de 2014 o programa não foi executado. Sobre os assuntos abordados nessas capacitações, foi informado que no ano de 2013 o programa apresentou o tema “Direito Digital com Enfoque em Segurança da Informação”, e no ano de 2015, será realizado uma capacitação denominada “Divulgação Política de Classificação do Sigilo e Confidencialidade de Informação”. Em relação ao cumprimento da política de segurança da informação, foi informado que a mesma dispõe de um Comitê de Segurança da Informação e Comunicação (CSIC), composto por representantes das unidades denominadas UTIC, unidade de assessoria jurídica (UAJ), unidade de gestão de pessoas (UGP), unidade de auditoria interna (AAI) e

diretoria executiva, cuja principal função está em assessorar a implementação das ações relacionadas à segurança da informação. Referente a existência de um canal para denúncias originadas de possíveis infrações na política de segurança da informação, ficou evidenciado que a mesma possui um canal de comunicação que é divulgado aos seus colaboradores e clientes, a fim de reportar os possíveis casos de incidentes de segurança da informação, dessa forma, o denunciante pode realizar a denúncia de modo formal ou com uso do recurso de denúncia anônima, sendo estes realizados através de e-mails ou contato telefônico. Sobre o questionamento de penalidades para o descumprimento da política de segurança da informação, foi exposto que quaisquer fatos relacionados a incidentes decorrentes da violação devem ser informados ao CSIC que irá verificar o caso e apurar as responsabilidades dos envolvidos através de procedimentos administrativos disciplinares, visando a aplicação de sanções administrativas apropriadas, uma vez que estas estão previstas em cláusulas contratuais e outros documentos normativos.

Sobre a rede própria para visitantes, mencionada anteriormente pelos entrevistados, ficou esclarecido que a mesma é referente a uma rede de internet denominada "wlan-visitante", onde os clientes e prestadores de serviços podem realizar o acesso através de uma identificação digital que utiliza o número do CPF do usuário, assim a unidade de tecnologia da informação e da comunicação pode realizar o controle de acesso.

Visando esclarecer as vulnerabilidades das informações empresariais através do uso de dispositivos móveis, foi discutido sobre o ato de ataques, como roubo de informações, originado por dispositivos móveis na organização, e diante do exposto, foi evidenciado por quatro colaboradores que a mesma foi vítima de um ataque denominado Spear Phishing, que tem como objetivo capturar dados particulares dos clientes. Durante esse ataque, 350 mil clientes foram afetados, pois o ataque expos informações relativas a alguns clientes da organização, capturando dados e posteriormente enviando uma comunicação eletrônica similar a oficial que teve como objetivo transferir códigos maliciosos para o computador da vítima e obter demais informações pessoais. Durante a pesquisa qualitativa, foi solicitado maiores detalhes sobre o fato, e afirmou-se que ocorreu há aproximadamente seis anos, através de um dispositivo móvel externo, identificado posteriormente pela unidade de tecnologia da informação e da comunicação. Porém, um dos colaboradores não informar sobre o caso, pois possuía pouco tempo de experiência na organização. Após a confirmação do ataque originado por dispositivo móvel e com o objetivo de esclarecer quais foram as ações realizadas a fim de combater a vulnerabilidade da organização em relação as informações empresariais, foi questionado sobre quais foram as ferramentas e estratégias

adotadas a fim de reforçar a segurança da informação e evitar possíveis novas ameaças, dessa forma, foi esclarecido que atualmente utiliza-se ferramentas especificas que visam proteger o ambiente empresarial de novos ataques, entre elas, estão Firewall; IPS e VPN do fabricante Juniper; Filtro de conteúdo McAfee e antivírus Sysmantec, além da atualização contínua da política de segurança da informação.

Nos resultados, pode-se fazer um parágrafo introdutório apresentando a estratégia utilizada para a subdivisão dos tópicos que serão tratados. Esta subdivisão auxilia na organização das ideias. Procure realizar subdivisões dos resultados quando houver grande número de variáveis. É aconselhado que esta subdivisão seja realizada de acordo com a natureza e relação entre as variáveis. Ou seja, coloque dentro de mesmos tópicos variáveis de mesma natureza e/ou que estejam relacionadas ao mesmo assunto da análise.

O objetivo principal deste tópico de "RESULTADOS" é apenas descrever os principais achados do estudo. Ou seja, aqui serão apenas apresentados os resultados obtidos por meio das coletas de dados realizadas. Procure dar a maior ênfase na descrição dos resultados para aspectos mais relevantes e que terão maior ênfase no próximo tópico do TCC (DISCUSSÃO). Deste modo, resultados que não estão ligados diretamente para responder ao problema de estudo, ou que não estão diretamente relacionados com as hipóteses de estudo levantadas, devem ter menor destaque neste tópico e na discussão posterior.

Os resultados podem ser apresentados por meio de diversas estratégias, tais como: utilizando a escrita discursiva (em texto), apresentando figuras, tabelas ou quadros. Durante todo o processo, no entanto, é possível que sejam resgatados autores mencionados no referencial teórico para corroborar, complementar, ou mesmo negar algum argumento. Por exemplo, ao descrever um resultado que se manifesta de modo semelhante a algo indicado no referencial, é possível utilizar expressões como "Tal resultado está de acordo com o que foi apresentado por Fulano (2000) ao mencionar que ...." . Ou então: "Tal resultado se apresentou de maneira distinta do que encontrado por Fulano (2000). Com base nisso é possível inferir que tal distinção pode ter sido ocasionada por tal e tal fator".

Em geral, esta seção pode ser dividida em subseções que possam facilitar a compreensão geral. O primordial, entretanto, é não perder de vista que esta trata de uma das principais partes do texto, na medida em que demonstrará como aquele argumento científico se constituiu em sua validade.

## 5 CONSIDERAÇÕES FINAIS

Os dados obtidos com a pesquisa de abordagem qualitativa demonstraram que a organização analisada está ciente da importância da segurança da informação e se mantém alerta sobre as tecnologias que permitem o rápido acesso, facilidade de mobilidade e troca de informações. De acordo com Moreira (2001), todos os ambientes computacionais são vulneráveis a incidentes de segurança e, portanto, à ação de ameaças, alguns com maior, outros com menor probabilidade de ocorrência, devido ao grau de eficiência das medidas de segurança implementadas. Consequentemente, pode-se afirmar que a organização analisada está vulnerável a ameaças em seus ambientes computacionais, apesar de possuir uma política de segurança da informação sólida e estruturada e entende-se que a correta gestão da segurança da informação ocorre quando a mesma é respeitada por todos os usuários a quem é aplicada, segundo artigo publicado por Felipe Cesar Damatto e Ricardo Rall (2010), sobre os possíveis motivos do aumento de incidentes de malwares nas empresas. Ficou evidenciado que na organização analisada, os 502 usuários que possuem acessos aos sistemas e ativos de tecnologia da informação têm obrigatoriedade em respeitar as normas e procedimentos descritos na PSTI, uma vez que assinam termos de compromisso passíveis de responsabilização, entretanto, pode- se afirmar não existe um rígido controle quanto ao cumprimentos das normas e procedimentos, principalmente quanto ao uso indevido da propriedade intelectual e divulgação de áudio, vídeos e fotos, fato que pode originar um possível vazamento de informações empresariais e comprometer a segurança da organização.

Para Miguel Maurício Isoni e Silvana Aparecida Borsetti Gregório Vidotti (2007), autores do artigo cientifico sobre as percepções de segurança e ameaças em ambientes de tecnologia da informação, as ameaças que comprometem o fluxo de informação precisam ser identificadas e ocorrem através da execução de códigos maliciosos e pela divulgação não autorizada de informações confidenciais, contudo, infere-se que durante a abordagem, foi comprovado que os incidentes de segurança da informação identificados na organização são avaliados por um Comitê de Segurança que instaura as responsabilidades dos envolvidos, dessa forma, incidentes originados do ambiente interno, ou seja, pelos usuários autorizados que utilizam os sistemas da organização, são identificados e recebem a responsabilização com base nas normas de violação ou tentativa de burla enunciadas na PSTI, conforme elucidado por Cansian (2001, p.144), onde afirma que “a origem de incidentes provenientes do meio interno, oriundos da própria organização, empresa ou instituição, e de atacantes externos, normalmente provenientes da Internet”. (CANSIAN, 2001, p.144).

Segundo os autores do artigo “Introdução à Segurança de Dispositivos Móveis Modernos – Um Estudo de Caso em Android” (2012), os dispositivos móveis são responsáveis pela mudança no mundo das tecnologias da informação e da comunicação, seja de uso pessoal ou profissional, devido ao grande poder de processamento e conectividade em ambientes públicos e privados. Para Rainer e Cegielski (2012), diferentes fatores contribuem para o aumento da vulnerabilidade das informações empresariais, e entre eles, pode-se citar o feito de que os computadores e dispositivos de armazenamento modernos estão cada vez menores, mais rápidos, mais baratos e mais portáteis, sendo assim, essas características facilitam o roubo ou vazamento de informações confidenciais. Diante disso, sabe-se que a organização analisada foi vítima de um ataque denominado Spear Phishing, realizado através de um dispositivo móvel externo, comprometendo aproximadamente 350 mil clientes, isto posto, evidencia-se que há seis anos a organização não estava preparada para anteceder e combater os casos de ataques remotos e originados por dispositivos móveis. Para Campos e Brito (2013), Spear Phishing são ataques que tem como objetivo fazer com que o utilizador acredite que a fonte do correio eletrônico é de confiança. Rainer e Cegielski (2012) definem Spear Phishing um ataque que visam grande grupos de pessoas, com o objetivo de descobrir o maior número de informações possíveis sobre as vítimas.

Foi notabilizado que após o ataque de Spear Phishing, nenhum outro ataque ocorreu na organização e ficou evidenciado que após o primeiro incidente a mesma adotou ferramentas que possuem o objetivo de combater possíveis novas vulnerabilidades. Francisco José Candeias Figueiredo e Paulo Lício de Geus (2011), autores do estudo sobre o acesso remoto em firewalls e topologia para gateways VPN, afirmam que essas tecnologias, como a VPN do fabricante denominado Juniper, disponibiliza o suporte necessário para garantir a privacidade da organização, protegendo as informações de alterações e ataques por parte de agentes não autorizados, além de permitir conexões seguras para usuários móveis. Contudo, conclui-se que a organização analisada já esteve vulnerável e comprometeu as informações empresarias, portanto, possibilitou a exposição de todo o seu conhecimento, método e estratégias acumuladas ao longo de sua história. Entretanto, após o incidente que foi registrado por ataque externo originado de dispositivo móvel, empregou-se o uso de ferramentas com o objetivo de minimizar os riscos com perdas, ataques ou violações, garantindo a segurança e continuidade do negócio. Moreira (2001), estabelece que a implementação de um sistema para gerenciamento e segurança da informação não reporta-se somente a instalação de softwares, mas também ao uso de outros dispositivos de controle e gestão para segurança da informação, sendo que entre eles pode-se citar análise de risco, política de segurança, controle de acesso

físico e lógico, treinamentos e conscientização para a segurança da informação, e plano de contingência. Já Pinochet (2014), afirma que as organizações precisam aderir a princípios que conduzam para a prática do gerenciamento ético da informação com base em atividades de conscientização e treinamento todos os colaboradores. À vista disso, foi evidenciado que a organização pode adotar outras ações para garantir e assegurar a segurança da informação, além de aprimorar as já existentes, reduzindo a vulnerabilidade das informações empresariais através do uso de dispositivos móveis.

A pesquisa de abordagem qualitativa demonstrou a vulnerabilidade das informações empresariais na organização analisada através de um ataque denominado Spear Phishing.

## REFERÊNCIAS

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

BRAGA, Alexandre Melo; NASCIMENTO, Erick Nogueira; PALMA, Lucas Rodrigues; ROSA, Rafael Pereira; **Introdução à Segurança de Dispositivos Móveis Modernos** – Um Estudo de Caso em Android. 2012.

CAMPOS, Pedro; BRITO, Pedro Quelhas. **Novas Tendências em Marketing Intelligence**. Coimbra: Actual. 2013.

CANSIAN, Adriano M. **Conceitos para perícia forense computacional**. Anais VI Escola Regional de Informática da SBC, Instituto de Ciências Matemáticas e Computação de São Carlos, USP (ICMC/USP), São Paulo. 2001.

DAMATTO, Felipe; RALL, Ricardo. **Estudo dos Possíveis Motivos do Aumento de Incidentes de Malwares nas Empresas**. São Paulo. 2010.