GABRIEL CORREA RICCI

GABRIEL DOS SANTOS LUZ

LUCAS SANTOS FERREIRA

BYOD E DLP: IMPLEMENTANDO SOLUÇÕES DE SEGURANÇA PARA PREVENÇÃO DE PERDA DE DADOS

SÃO CAETANO DO SUL/SÃO PAULO

2020

GABRIEL CORREA RICCI

GABRIEL DOS SANTOS LUZ

LUCAS SANTOS FERREIRA

BYOD E DLP: IMPLEMENTANDO SOLUÇÕES DE SEGURANÇA PARA PREVENÇÃO DE PERDA DE DADOS

Trabalho de conclusão de curso apresentado à Faculdade de Tecnologia de São Caetano do Sul, sob a orientação da professora Msc. Edna Mataruco Duarte, como requisito parcial para a obtenção do diploma de Graduação no Curso de Tecnologia em Segurança da Informação.

SÃO CAETANO DO SUL/SÃO PAULO

2020

Resumo

LUZ, Gabriel; RICCI, Gabriel; FERREIRA, Lucas. **Estudo da adoção corporativa do BYOD: Implementando soluções de segurança para prevenção de perda de dados**. 51 f. Trabalho de Graduação – Faculdade de Tecnologia de São Caetano do Sul, 2020.

Diante das constantes e rápidas mudanças tecnológicas que interferem no modo como as pessoas vivem e se interagem, faz se necessário que as organizações estejam atentas para também se adaptarem as novas formas de comunicação e de como todos estão se relacionando. É possível ver isso com o grande crescimento de aquisições dos dispositivos pessoais como *smartphones*, *notebooks* e *tablets.* As pessoas hoje carregam esses dispositivos como se fossem uma extensão de suas vidas, consequentemente, interfere a forma como trabalham e isso provoca transformações dentro das organizações. Essa prática é conhecida como *Bring Your Own Device* - BYOD. Apesar de trazer vantagens como redução de custos, maior conforto e aumento na produtividade dos funcionários, essa atividade abre diversas brechas que podem resultar em perda de dados e informações que são críticas para o funcionamento dos negócios. Diante do exposto, é de extrema importância realizar análises destas informações, da infraestrutura tecnológica e dos processos de negócio para que se faça a implementações de controles e segurança com o propósito de mitigar os possíveis vazamentos, perda e/ou roubo de dados. Diante deste cenário este trabalho de conclusão de curso tem como objetivo elencar algumas soluções de segurança na implantação do BYOD com o DLP, buscando contribuir com a mitigação de riscos em diferentes organizações. Trata-se de pesquisa descritiva de natureza qualitativa. Com isso busca abordar o tema e propõe algumas das possíveis soluções que podem ser implantadas nas organizações para a obtenção de uma maior segurança das informações sensíveis.

Palavras-chave: Segurança da informação, BYOD, DLP

Abstract

LUZ, Gabriel; RICCI, Gabriel; FERREIRA, Lucas. **Estudo da adoção corporativa do BYOD: Implementando soluções de segurança para prevenção de perda de dados**. 51 f. Trabalho de Graduação – Faculdade de Tecnologia de São Caetano do Sul, 2020.

Given the fast and constant technological changes that directly interferes in the different ways that people live and interact with each other, creating the need for companies and organizations to be always updated and prepared for new ways to interact with the standard workplace and their communications. This necessity becomes evident with the increase in the acquisition of devices like smartphones, laptop computers and tablets for personal use. Today people carry those devices as if it were an extension of their own bodies, and consequently, changing the work dynamics in these companies. Today, this practice is known as BYOD (short for Bring Your Own Device). While this practice can offer advantages like cost reduction, comfort for employees and increase in productivity, it also brings vulnerabilities to the organization, resulting in data loss of the company's critical information. Considering this scenario, it is extremely important to beforehand analyze those pieces of information, the technological infrastructure, and the business processes, to properly implement security controls, reducing leaks, loss, or theft of data. Having this situation in mind, this final paper has the objective of pinpointing available security solution for a safe implementation of a Bring Your Own Device workplace with Data Loss Prevention, with the sole objective of keeping the risks of different organizations at their minimum. Being a descriptive research of qualitative nature, this paper seeks to address the theme, and offers possible solutions that can be implemented at companies, with the goal of achieving better security for their sensitive information.

Keywords: Information security, BYOD, DLP

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AWS *Amazon Web Services* (Plataforma de computação em nuvem da Amazon)

DLP *Data Loss Prevention* (Prevenção de Perda de Dados)

BYOD *Bring Your Own Device* (Traga seu Próprio Dispositivo)

CYOD *Choose Your Own Device* (Escolha seu Próprio Dispositivo)

GCP *Google Cloud Computing* (Plataforma de computação em nuvem da Google)

GDPR *General Data Protection Regulation* (Regulamento Geral de Proteção de Dados)

HIPAA *Health Insurance Portability and Accountability Act* (Lei de portabilidade e responsabilidade do seguro de saúde)

ISO 27001 Padrão e referência internacional para a gestão da Segurança da Informação

PCI DSS *Payment Card Indsutry Data Security Standard* (Padrão de Segurança de dados da Indústria de Pagamento com cartão)

Sumário

Introdução

À medida que a tecnologia avança, surgem no mercado novidades que afetam e influenciam as empresas proporcionando transformações contextuais. Ao revisitar a história, desde as grandes revoluções, industrial, elétrica e o aumento da competitividade entre as empresas, é constatável a importância da informação dedicada ao empreendimento. Independentemente do tipo de negócio, seja ele um supermercado, instituição bancária ou indústria, em todos os contextos, a informação está intrínseca nas decisões e planos caracterizando um diferencial competitivo, resultando no crescimento e continuidade do negócio (SÊMOLA, 2003, p. 1).

Diante deste cenário de mudanças, cada vez mais as empresas estão admitindo a prática do *Bring Your Own Device* (BYOD) que tem representado de muitas maneiras o futuro dos locais de trabalho, abandonando progressivamente a imagem antiga da filiação dos empregados e os escritórios. Aliado a este fato, as novidades tecnológicas cada vez mais presentes no cotidiano, como as conexões 4G, WI-FI possibilitam a execução das atividades em diversos outros dispositivos que melhor atendam às necessidades do empregado. (KEEPER, 2016, p.3).

Apesar de apresentar novidades que trazem benefícios, esta prática também carrega alguns pontos em que se faz necessário um cuidado adicional. Segundo a Ernst & Young (2011, p.1), a prática do BYOD impacta significativamente os modelos tradicionais de segurança e proteção da Tecnologia da Informação, necessitando aplicar uma nova postura e novos procedimentos que possibilitam abranger as necessidades dos empregados e a segurança de dados.

É oportuno criar e gerenciar previamente, controles de segurança interna representando uma camada primária a segurança de dados composta por implementações de soluções de segurança e controle como: *firewall*, *proxy*, sistema de detecção de intrusão e políticas de segurança.

Ao averiguar que BYOD possui complicações quanto a segurança de dados sensíveis, a presente pesquisa tem o intuito de responder: As soluções DLP junto com as ferramentas de controle de segurança são eficazes na prevenção de perda, vazamento e compartilhamento indevido de informações?

Diante deste cenário, o presente estudo tem como objetivo elencar algumas soluções de segurança na implantação do BYOD com o DLP, buscando contribuir com a mitigação de riscos em diferentes organizações. Dessa maneira, é importante informar que existem outras soluções que auxiliam na mitigação de perda e vazamento de dados, mas que nesta pesquisa não serão tratados a fundo.

Um estudo realizado pela instituição certificadora de TI, CompTIA (2014), diz que 53% das empresas norte americanas não permitem que funcionários tragam seus dispositivos pessoais para utilizar na empresa, tendo como motivações: a necessidade de aprimoramento tecnológico (43%), a necessidade de centralizar o controle de segurança (35%), e a despreocupação dos usuários com segurança (31%).

Já dados fornecidos pelo Ibope Conecta (2017), 54% das empresas em território nacional admitem a utilização de computadores pessoais de seus funcionários. Olhando financeiramente, só há vantagens, pois, os custos serão pagos pelo próprio funcionário, e por ele ser o proprietário do aparelho, estará familiarizado com o próprio ambiente de trabalho, o que ajuda na resolução de problemas, e que também tem certo impacto na produtividade. Vale ressaltar o momento de pandemia vivido em todo mundo no ano de 2020, onde grande parte das empresas adotaram, em alguns casos, o trabalho de forma remota, reforçando ainda mais a tendência de mudança na maneira de se trabalhar.

O maior desafio do BYOD é a segurança dos dispositivos e das informações da empresa nele contido. Portanto, justificamos uso de ferramentas de segurança e controle de fluxo de informação para o acesso em ambiente micro/macro empresarial e analisar o ambiente onde se insere o BYOD, com o intuito de identificar problemas de perda e vazamento de informação em meio corporativo.

Nesse estudo utilizaremos a pesquisa descritiva de natureza qualitativa, tomando como base um estudo a partir de fontes secundárias e com o objetivo de se obter conhecimento sobre o BYOD desde o surgimento, aceitação por parte das organizações, pontos positivos e negativos. A partir deste panorama, serão apresentados os riscos envolvidos, elencando soluções de segurança para mitigar as ameaças internas e por fim, mostrar algumas soluções de DLP a fim de prevenir a perda de dados.

1 Segurança da Informação

A Segurança da Informação pode ser entendida como um campo do conhecimento que se dedica a proteger os ativos da informação contra alterações indevidas, acessos não autorizados ou indisponibilidade do mesmo. Ela também pode ser interpretada, de uma forma mais abrangente, como uma atividade de gestão de riscos e incidentes que resultem em três principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação (SÊMOLA, 2003, p. 43).

É importante que se entenda e seja apresentado de forma clara cada um desses elementos que foram citados e que compõe a área de principal estudo neste trabalho. Conforme escrito também por Sêmola (2003), existem conceitos básicos que orientam a implementação da prática, são eles:

- Confidencialidade como toda informação deve ser protegida conforme o nível do sigilo de seu conteúdo, assim, restringe o acesso somente a pessoas que são devidamente destinadas.
- Integridade sendo toda informação que deve ser velada na mesma condição que foi viabilizada através de seu proprietário, com o objetivo de resguardar contra alterações indevidas, intencionais ou acidentais.
- Disponibilidade referindo-se a toda informação criada ou obtida por um indivíduo ou instituição deve estar à disposição de seus usuários no instante em que forem requisitadas para qualquer que seja a finalidade.

A segurança é um termo que pode ser interpretado de duas maneiras, sendo, segurança como “meio”, que se propõe a garantir a confidencialidade, integridade e disponibilidade da informação. A segurança como “fim”, que é obtida através de políticas e práticas adequadas dentro de uma padronização gerencial e operacional dos ativos e processos que manipulam a informação (SÊMOLA, 2003, p. 44).

Informação pode ser entendida como um conjunto de dados que são manuseados em transferências de mensagens entre indivíduos ou máquinas que estão enquadradas em contextos comunicativos, ou inseridas em processos transacionais. A informação está presente e é manipulada por diversos ativos, este qual é um alvo que a segurança da informação visa proteger (SÊMOLA, 2003, p. 44).

Ja o ativo, é todo componente que integra os processos que manuseiam e processam a informação, os equipamentos no qual ela é armazenada, manipulada, transportada e descartada. É uma parte considerada com grande valor para um indivíduo ou organização, e devido a isso necessita de proteção adequada (SÊMOLA, 2003, p. 44).

Além dos conceitos básicos, o mesmo autor apresenta alguns aspectos da segurança da informação que são encarados como essenciais e de relevância para o estudo deste trabalho.

A ameaça trata de circunstâncias ou agentes que provocam incidentes colocando as informações e os ativos envolvidos em risco por exploração de brechas, onde há a possibilidade de comprometimento da confidencialidade, integridade e disponibilidade. Elas podem ser classificadas como Naturais: ligadas aos fenômenos da natureza, como enchentes, incêndios, terremotos, poluição. Involuntárias: causadas quase em todas as vezes por desconhecimento, falhas e acidentes. Voluntárias: ocasionadas propositalmente por humanos, como *crackers*, espiões, ladrões disseminadores de vírus (SÊMOLA, 2003, p. 47).

Sêmola (2003), também define que a vulnerabilidade é a fraqueza presente nos ativos que manipulam e/ou processam as informações, na qual se for explorada pelas ameaças, ocasionará um incidente de segurança, e é de importancia ressaltar que a vulnerabilidade necessita que um agente provoque uma condição para que ela seja explorada, sendo assim, ela é um elemento passivo. Este aspecto também é classificado em algumas categorias como:

- Físicas: Instalações prediais mau construídas ou mau planejadas, ausência de extintores, detectores de fumaça, câmeras, entre outros.
- Hardware: Falha dos equipamentos tecnológicos.
- Software: Erros de configuração que podem acarretar em acessos indevidos, roubo ou vazamento de informações e indisponibilidade do serviço.
- Humanas: Desconhecimento de boas práticas, não efetuação das rotinas de segurança, compartilhamento indevido de informações, erros operacionais, roubos de dados.

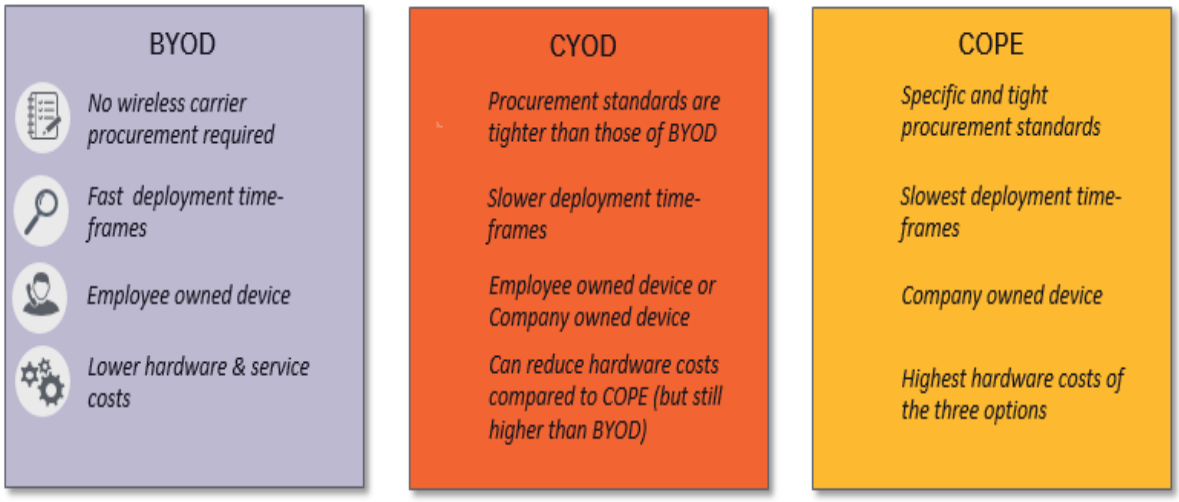
Os tópicos foram apresentados com o propósito de criar uma base conceitual e nortear o leitor ao principal tema discutido, a prevenção da perda de dados na implementação do BYOD. Diante desse exposto, o princípio da confidencialidade será abordado com maior ênfase no decorrer deste trabalho.

2 Panorama acerca do BYOD

Segundo a Forcepoint (2019), o *Bring Your Own Device* (BYOD) se refere a uma tendência que funcionários utilizem os dispositivos pessoais para se conectar às redes organizacionais, tendo acesso à sistemas relacionados ao trabalho e dados potencialmente sensíveis ou confidenciais por meio desse dispositivo. O cenário abrange: *smartphones*, computadores pessoais, *tablets* e unidades USB de armazenamento). Conforme apresentado por French, Guo, Shim (2014, p.2) há uma predisposição pelas organizações em acolher a prática do BYOD visto que os dispositivos inteligentes têm gradativamente invadido a vida pessoal das pessoas a ponto de serem uma extensão das mesmas, ou seja, são profundamente inerentes aos comportamentos pessoais, preferências e a realização das atividades rotineiras de cada uma.

Existem vantagens nítidas em relação a essa prática: (1) os empregados são mais familiarizados com seus próprios dispositivos; (2) as empresas são beneficiadas com reduções de custo porque não precisam adquirir novos dispositivos para o exercício das atividades de seus empregados e (3) permite o desenvolvimento da flexibilidade, conveniência, portabilidade dos equipamentos, maior inovação e a produtividade é ampliada na execução dos trabalhos. Também existe a possibilidade da empresa especificar quais os dispositivos que poderão ser permitidos, conhecido como *Choose Your Own Device* (CYOD), ou ainda, disponibilizar temporariamente para o empregado um dispositivo pré-configurado para utilizar tanto no trabalho como em assuntos pessoais, que é conhecido como *Corporate-Owned Personally-Enabled* (COPE), a Figura1 aponta os principais pontos de cada prática.

Figura 1: BYOD vs CYOD vs COPE



Fonte: Calero (2019)

Apesar de apresentar vantagens às organizações e seus funcionários, a segurança deve ser tratada como prioridade, com possibilidade de adotar por uma abordagem passiva ou ativa. A abordagem passiva simplesmente aceita que os funcionários façam o uso dos dispositivos, e na ativa, é criada uma política para o BYOD que é implementada no ambiente de trabalho (FRENCH; GUO; SHIM 2014, p.3). É impreterível se atentar para as tecnologias *smart*, que tem impactado a forma com que as pessoas se comunicam e se relacionam com a variedade de serviços oferecidos. A adequação a essas tecnologias nos ambientes de trabalho iniciou-se na invenção do *Blackberry*, obtendo grande popularização da aquisição e emprego dessa tecnologia com os *Iphones* e dispositivos *Android* que por conseguinte trouxe o emprego do *Bring Your Own Device* (FRENCH; GUO; SHIM 2014, p.3). Em uma pesquisa realizada em 2013, o fenômeno foi tão impactante que cerca de 71% das empresas ao redor do mundo alteraram ao menos um processo para se adaptar ao uso de dispositivos pessoais de seus colaboradores (QING, 2013).

Em 2013, Joseph M. Bradley da Cisco, companhia de tecnologia provedora de soluções de rede e Internet, através de uma pesquisa constatou que houve confirmação por meio de uma análise financeira através de seis países, dentre eles: Brasil, China, Alemanha, Índia e Estados Unidos, em que se nota valores significantes na adoção deste novo conceito de trabalho.

- Os empregados ganharam em média, cerca de 37 minutos de produtividade por semana. Esse dado varia entre os países da pesquisa, enquanto nos Estados Unidos os funcionários ganharam 81 minutos por semana, na Alemanha apenas 4, onde o BYOD é visto de forma mais cética.

- Na época, a adoção do *Basic* BYOD, que é um nível de implantação mais simples, gerou em média 350 dólares de valor positivo para cada dispositivo móvel.

- O smartphone é a opção de maior proporção, e que cada funcionário havia pagado cerca de 965 dólares por eles.

Bradley (2013) informa que a eficácia nos custos da implementação do BYOD necessita de maturidade das práticas, políticas e de uma implementação ideal chamada *Comprehensive* BYOD, traduzido como BYOD abrangente, que possibilita elevar o nível dos benefícios para a organização. Poucas empresas estão próximas de uma maturidade ideal que atingem o conceito maturado. O potencial de ganho de uma implementação “básica” para uma “abrangente” é visivelmente alto.

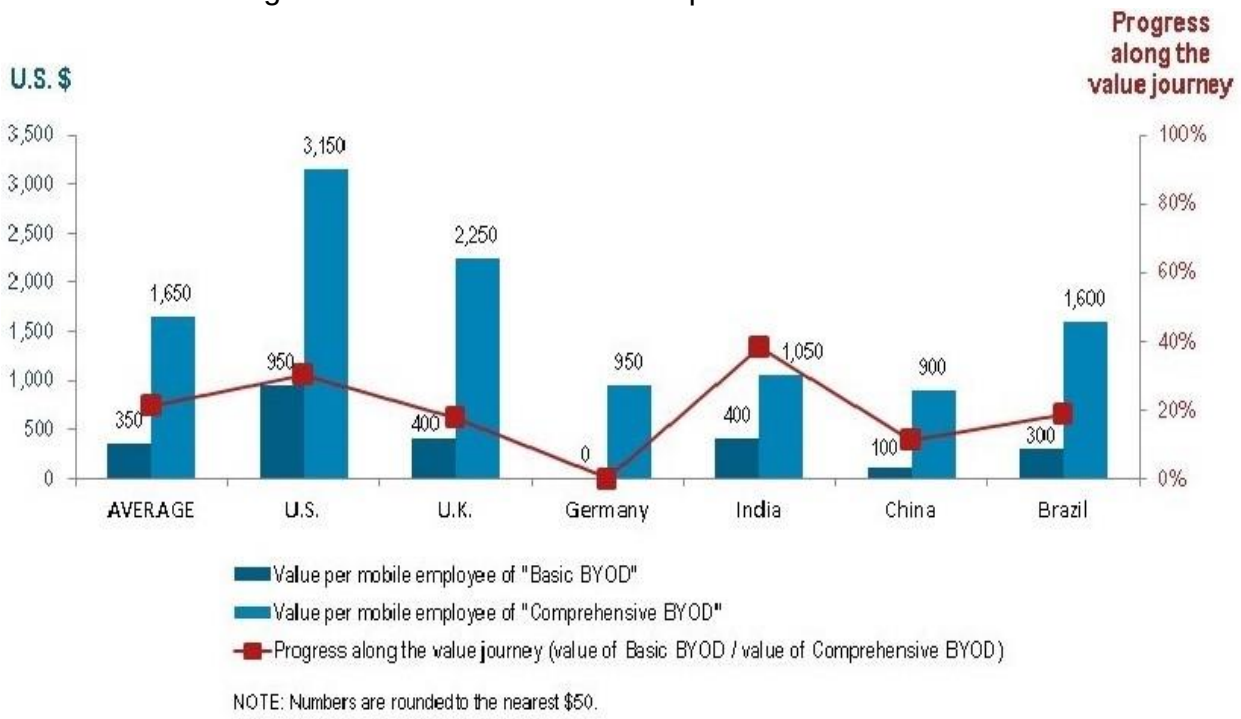
- Com a adoção do *Comprehensive* BYOD as organizações podem ter um ganho anual de 1.650 dólares para cada dispositivo móvel de cada funcionário.

- As companhias norte americanas podem ganhar ainda mais a partir dessa prática de implementação ideal. Para cada dispositivo de cada um dos empregados, o aumento anual sobe de 950 para 3.150 dólares.

- Os funcionários potencializaram suas capacidades de inovação, e a partir da efetuação da prática abrangente, houve um acréscimo de 17% de produtividade.

Na Figura 2 podemos visualizar, através dos gráficos, uma comparação de valores financeiros entre o *Basic* BYOD e o *Comprehensive* BYOD:

Figura 2: Basic BYOD and Comprehensive BYOD



Fonte: Bradley (2013)

De acordo com um estudo feito pela empresa de consultoria Ernst & Young (2017), apesar de trazer aumento da produtividade e até mesmo uma maior satisfação do próprio empregado, há claramente ameaças à segurança envolvidas que podem resultar em danos incomensuráveis. O advento dos dispositivos móveis nos ambientes de trabalho estimulou o crescimento dos crimes cibernéticos dos quais a escala é muito grande.

A seguradora britânica *Lloyd's* estimou que estes crimes resultam em 400 bilhões de dólares aos negócios todo ano. Em um fórum mundial da economia na cidade suíça de Davos, o assunto de destaque se referiu a segurança cibernética, foi dito pelo CEO Pierre Nanterme da empresa de consultoria Accenture, que os maiores problemas enfrentados pelos negócios será a segurança (GANDEL, 2015).

A expansão da tecnologia dentro das companhias afeta também as empresas de menor porte, que também devem adotar políticas para os dispositivos móveis. O risco de crime cibernético sendo pequeno, médio ou grande, em todo tipo de organização, deve seguir uma regra simples: autorizando o uso dos dispositivos móveis pelos empregados para fins de trabalho, essas organizações necessitam

compreender as ameaças envolvidas e se anteciparem para implementar proteções adequadas com suas realidades (KEEPER, 2016, p.3).

Diante desse cenário, foi possível compreender os principais aspectos do BYOD, como foi incorporado pelas organizações ao longo do tempo, alguns benefícios e riscos envolvidos.

2.1 Análise de ambiente corporativo interno

Após a apresentação da visão panorâmica do BYOD, suas vantagens e riscos envolvidos, o estudo seguirá neste tópico focado em apresentar alguns problemas que podem afetar a segurança interna da empresa.

Os funcionários mesclam suas vidas pessoais e profissionais em seus dispositivos, e devido a isso, podem involuntariamente expor dados sensíveis ou criar vulnerabilidades para ataques cibernéticos. Infelizmente, os ataques são oportunistas, e cedo ou tarde, vulnerabilidades em aplicações *mobile* e sistemas operacionais irão usufruir dessas brechas. Em 2015 foi realizado um monitoramento através do IBM Trusteer em dispositivos móveis e as infecções por *malwares* neste tipo de equipamento, em termos de quantidade, foram iguais aos computadores convencionais. Através dos estudos realizados pela inteligência de segurança da IBM em 2018, o aumento das infecções em dispositivos móveis se deu principalmente mediante ao *Marcher malware*, que é uma combinação de *phishing* (e-mails fraudulentos) e vírus cavalo de Tróia. Por meio deste tipo de ataque, dispositivos de milhões de pessoas foram infectados, e informações de empresas comprometidas (IBM, 2019).

Um outro estudo, realizado pela empresa especializada em segurança, Keeper em 2016, ainda cita alguns riscos envolvidos na prática do BYOD.

- *Download* de aplicativos: A maior parte dos usuários de aplicativos em dispositivos móveis desconhece os perigos dos *malwares*[1] que podem estar presentes. Eles conseguem providenciar medidas de segurança em seus

[1] *Malware* é um termo genérico para qualquer *software* malicioso projetado para infiltrar o dispositivo sem o devido conhecimento. (AVAST, 2020).

desktops e *notebooks,* porém o mesmo não acontece em *tablets* ou *smartphones.* É interessante pensar que essa mentalidade é alterada quando ocorre algum tipo de ataque, como por exemplo, em fevereiro de 2015, onde o Google precisou remover 3 aplicativos de sua loja porque possuíam *software* malicioso.

- *WiFi* inseguro: Quando se adota uma política para o uso dos dispositivos, em muitos dos casos, as empresas se esquecem que os equipamentos em sua maioria os *smartphones* e *tablets*, se conectam às redes sem fio de outros locais. Os usuários raramente pensam sobre onde estão conectando e que o seu dispositivo pode ser *hackeado* ou infectado por algum *software* malicioso, assim, ao retornar a rede da empresa, o próprio dispositivo funciona como um cavalo de Tróia.

- Descuido dos empregados: Há muitos riscos envolvidos nessa categoria. Quando uma organização não é proprietária do equipamento, é difícil convencer que os empregados tenham boas práticas como: instalação de atualizações de segurança, restrição de acesso de aplicativos a dados pessoais e não “subir” arquivos e dados para os serviços em nuvem.

  Estes são alguns descuidos que podem ser utilizados como uma porta para invasões de agentes maliciosos ou perda de dados.

- Empregados mal-intencionados: Podem ocorrer situações em que os empregados queiram intencionalmente prejudicar a empresa sendo elas: instalação de *softwares* com o propósito de roubar informações, ter acessos privilegiados e afetar o funcionamento dos sistemas.

Adicional a essas, a vice presidente de *Marketing* da CCB *Technology*, Melody Bernhardt cita um ponto que deve ser levado com muita seriedade.

- Ausência de treinamento adequado: Um empregado que não possui pleno conhecimento e orientação das políticas internas da empresa, automaticamente gera uma vulnerabilidade. Isso se torna mais preocupante ao verificar que menos da metade das empresas que fazem prática do BYOD possuem uma política específica para este fim em vigor.

A Lucidchart (2019) com profissionais de diversas áreas correlacionadas a TI (setores de finança, educação, governamental, telecomunicações, entre outras), elucidou as seguintes informações referentes ao funcionamento do ambiente interno de uma organização atualmente:

- Em desafios para a empresa, estavam inclusos realização de trabalho remoto e políticas para dispositivos (realização remota de trabalho representam dificuldades para 56% dos entrevistados, e políticas para dispositivos 46%).
- Em 2017, foi reportado que 36% dos empregados trabalhavam a distância, já em 2019, esta porcentagem subiu para 45% e está previsto subir para 54% nos próximos 2 anos.
- Dos entrevistados, em média, *Windows* é utilizado por 55% dos empregados, seguido pelo Mac, com 26% e Linux com 19%.
- 48% das organizações entrevistadas utilizam de políticas BYOD ou CYOD.

Um outro ponto importante a se considerar, são os roubos de dados por parte dos funcionários quando são desligados da empresa. Um estudo feito pela empresa Biscom (2015), informa que mais de 25% dos funcionários praticam este delito. Opsitnick, Anguilano e Tucker (2019) realizaram uma experiência onde certificou-se que quando ocorre este tipo de incidente, estão envolvidos: lista de clientes, fórmulas secretas, código-fonte, documentos estratégicos e segredos comerciais. São usadas contra a organização de forma que o ex-funcionário possa abrir uma nova empresa ou repassar a algum concorrente. Há indicações de atividades anormais que são constatadas por peritos forenses em uma investigação, e incluem:

- Evidências de conexão de dispositivos USB, como pen drive e disco rígido
- Conexões remotas durante dias de folga ou horários fora do expediente
- Transferência de grandes quantidades de dados na rede
- Envio de e-mails com anexos para contas pessoais

Além disso, é possível saber quais foram os arquivos acessados e possivelmente transferidos através de recursos que o próprio sistema operacional disponibiliza, desta maneira, há mais propriedade para a constatação do roubo de informações.

2.2 Análise de ambiente corporativo externo

Após a escolha de se usar uma política de BYOD no ambiente corporativo, o meio externo torna-se um risco para os dados de uma corporação pois, implica em diversos dispositivos de diversas versões, os quais, podem conter dados de uma empresa. Além de catalogar os dispositivos dos empregados, é necessário o uso de estratégias para impedir o vazamento dos dados. Através da detecção de brechas que podem causar a perda de informação sensível da corporação, bloqueando o uso de dados sensíveis a todo o momento (BURNHAM, 2014).

A Ernst & Young (2011), através de uma análise, informou que um dos problemas mais comuns relacionados a segurança de dados envolve: perda física do equipamento, divulgação acidental ou proposital e transmissões eletrônicas. Em muitas situações, os usuários não possuem a consciência adequada dos riscos envolvidos ao enviar informações através de *e-mails* sem criptografia, mensageiros instantâneos e ferramentas de transferência de dados.

Além disso, para Ernst & Young (2011), o desenvolvimento tecnológico aumentou rapidamente o crescimento do volume de dados e, consequentemente mais riscos foram incrementados, como por exemplo, o uso massivo de dispositivos móveis, como citado anteriormente neste estudo, que facilitam o acesso a dados sensíveis. Um caso envolvendo a *Wikileaks* mostrou que a segurança externa é tão ou mais importante que a interna. Um ex-funcionário de um banco suíço, vazou dados de mais de 2000 indivíduos expondo sonegação de impostos, o que anuncia mais uma vez que empregados com acesso a dados críticos colocam as organizações em risco, denegrindo a imagem delas.

Dessa maneira, a externalização do ambiente de BYOD traz consigo desafios e ameaças a serem consideradas:

- Roubo de dispositivos: Para Bernhardt, um dos riscos mais fáceis de ocorrer, e isso é agravado quando os proprietários não usam senhas para acesso. Um smartphone sem um código de acesso, ou com senhas fáceis de serem descobertas, conectado aos sistemas da empresa é um desastre iminente para acontecer. De acordo com Okyle (2015), editora do site Etrepreneur, 90% dos empregados possuem senhas que podem ser hackeadas em seis horas, além

disso, 65% dos adultos nos Estados Unidos utilizam a mesma senha para todas suas contas.

- *Mobile:* Ernst & Young (2011), informa que a facilidade de conectividade à Internet e redes sociais, propicia a divulgação e compartilhamento de informações facilitando ataques cibernéticos.
- Empregados mal-intencionados: Ernst & Young (2011), revela também o alto risco que pode causar grandes perdas financeiras e de reputação para empresa, como por exemplo, um funcionário que ao saber de sua demissão previamente, acessa um arquivo importante de um cliente, exporta as informações para um arquivo de Excel e o envia para o seu endereço de *e-mail* pessoal.

Além desses, a (McAfee 2017), cita mais algumas ameaças, entre elas:

- Funcionário envia arquivos para nuvem que está sincronizada a um diretório em uma máquina local.
- Infecção por *malware* enviado através de *phishing (*técnica de envio de e-mail ou mensagens mal-intencionadas) com objetivo de obter acesso não autorizado.
- Códigos maliciosos: Esse caso é o mais sofisticado dos que já foram citados anteriormente. Uma aplicação que foi instalada legitimamente, por alguma situação, possui um código malicioso que executa funções que resultam em vazamento de dados.

Por conseguinte, conclui-se até então, que as organizações tenham plena ciência de que estão vulneráveis com a perda de dados se permitirem sem qualquer inspeção, o uso de dispositivos de propriedade de seus empregados, portanto, se faz necessário implementações de políticas, controles e ferramentas para proteção e prevenção de vazamento de dados.

Algumas das soluções já comumente utilizadas em algumas empresas auxiliam muito a manter seus ambientes seguros, neste caso, apresentaremos brevemente algumas delas, e posteriormente no Quadro 1 como elas podem ser úteis contra algumas ameaças.

Segundo a empresa NTTSecurity (2019), *Endpoint Security Services* também conhecido como ESS, é uma solução amplamente recomendada contra ameaças do BYOD e que possui basicamente três funções integradas.

1. Monitoramento: Inclui monitoramento de conformidade, práticas recomendadas de políticas e segurança. Realiza coleta de dados, tendências e oferece alertas personalizados, relatórios com orientações de boas práticas
2. Detecção: Possui a combinação de detecção e análise avançada de ameaças, inclui recurso de aprendizagem de máquina, utiliza a função de monitoramento em tempo real para correlacionar o emparelhamento da rede e os serviços em nuvem. É capaz de exibir relatórios, resumo de eventos com ações corretivas.
3. Resposta: Recurso composto a aderir a conformidade de segurança, gerenciamento de políticas, isolamento de dispositivos potencialmente comprometidos.

Mobile Device Management (MDM) é um software que permite controlar e implantar políticas de segurança em dispositivos móveis como *smartphones* e *tablets*. Esta solução inclui gerenciamento de aplicações, gerenciamento de acesso e controle de sincronização e compartilhamento de arquivos (ROUSE, 2020).

Anti Malware: Software capaz de monitorar um computador ou rede afim de conter incidentes de segurança, detectando, identificando, bloqueando e removendo *malwares* (MYCYBERSECURITY, 2016).

2.3 Ameaças associadas à prática do BYOD

Quadro 1: Soluções propostas

Ameaça	Solução/Orientação
Utilizar os dispositivos em redes sem fio públicas	ESS possuem a capacidade de criptografar os dados que serão transmitidos pela rede, como *e-mails*, chamadas e mensagens de texto.
Perda, roubo ou descarte inapropriado do dispositivo	Utilizar um *software* de MDM para realizar a limpeza de todos os dados presentes no dispositivo.
Bugs ou incompatibilidades com o sistema operacional.	Utilizar um *software* MDM para acompanhar as versões do sistema

	operacional e aplicar a atualização quando atualizações forem lançadas.
Aplicativos defeituosos ou maliciosos	Utilização de softwares de (ESS) nos *Endpoints*[2] que conseguem monitorar e gerenciar aplicativos instalados.
Phishing e ataques direcionados ao usuário	Os MDM podem bloquear a instalação de aplicativos mal intencionados em dispositivos móveis. Enquanto as ESS oferecem a *desktops* e *notebooks,* ferramentas *anti malware*, monitoramento de comportamento e proteção a vulnerabilidades e *exploits*[3] de navegadores web.
Política inexistente/ineficiente	Manter a política de BYOD da empresa com o maior número de detalhes possíveis, especificando o estado e quais dispositivos poderão ser utilizados, as responsabilidades do empregado, e o que as soluções implementadas irão proteger.
Rooting[4]*/Jailbreaking*[5]	Existem MDMs que conseguem identificar dispositivos móveis que possuem acesso administrativo ou passaram pelo processo de *jailbreak*, porém não é recomendado manter estes dispositivos, já que foram desativados recursos de segurança implementados pelo próprio fabricante.

Fonte: Autoria própria

[2] *Endpoint* é um dispositivo remoto que realiza comunicação com a rede na qual está conectado, e pode ser: computador, *laptop, smartphone, tablet* ou servidor (PALOALTO, 2020).

[3] *Exploit* é um software malicioso com capacidades de explorar vulnerabilidades de um dispositivo local ou remoto (KASPERSKY, 2016).

[4] *Rooting* é um processo que permite obter permissões de administrador de sistema sobre um dispositivo, assim é possível realizar modificações no sistema operacional, aplicativos e configurações (BILIC´, 2016).

[5] *Jailbreak* também traduzido por “fugir da prisão” é uma técnica que permite a instalação de aplicativos que não se encontram disponíveis nas lojas oficiais das fabricantes dos sistemas operacionais (BILIC´, 2016).

3 Data Loss Prevention

Até o momento foi apresentado o BYOD, os benefícios e riscos associados no que se refere a perda de dados sensíveis a uma corporação. Felizmente uma solução tecnológica eficaz surge com o propósito de trazer mais segurança e refrear possíveis perdas ou roubo de dados, o *Data Loss Prevention* (DLP).

Conforme estudo feito pela Ernst & Young (2011), o DLP é definido como uma prática de detecção e prevenção de vazamento de dados confidenciais para o uso não autorizado, assim, os dados podem ser englobados como físicos ou digitais, e os mesmos podem ter sido vazados de forma intencional ou não, de modo que, antes de se realizar a implementação dos controles dessa tecnologia de forma eficaz, a organização deve compreender e responder três perguntas fundamentais: quais dados sensíveis são mais importantes, onde estão seus dados sensíveis e para onde estes dados estão indo.

1. Quais dados sensíveis são mais importantes?

Os dados devem ser classificados de uma perspectiva de negócio, isso quer dizer que além de rotular como confidenciais, secretos, sensíveis e públicos, a organização deve compreender e especificar os tipos de dados que devem ser mantidos seguros, e assim o DLP pode ser customizado e aplicado as necessidades específicas do negócio.

Não há uma abordagem única que descreva quais dados são importantes, porque isso irá depender do tamanho e tipo de cada organização, entretanto, deve-se considerar os dados dos processos críticos do negócio, tornando-se assim mais claro o que não pode ser perdido. Somado a estes pontos, também é necessário considerar uma avaliação de riscos para cada tipo de dado como: (1) a regulação para proteção de dados; (2) o impacto gerado aos clientes e parceiros de negócio e (3) impacto na marca e reputação, competitividade e vantagens de negócio.

Exemplos de alguns dados que possivelmente podem ser considerados: fórmulas, propriedade intelectual, dados pessoais de empregados, pagamentos bancários, status de pagamento e balanço contábil.

2. Onde estão os seus dados sensíveis, internamente, com terceiros ou em ambos?

Os dados podem estar armazenados em diversos lugares da infraestrutura de TI da organização, e isso irá decorrer de como os negócios são conduzidos. Os dados sensíveis podem estar em servidores, estações de trabalho, compartilhados na rede interna, dispositivos móveis, mídias e em nuvem. Após o mapeamento dos lugares onde estão os dados sensíveis, os responsáveis poderão começar a analisar sua infraestrutura de TI, atentos a dois dos principais pontos de onde esses dados estarão armazenados:

- **Repositórios estruturados:** Os dados estarão estruturados como em banco de dados relacionais que são tipicamente suportados e controlados pela TI da organização.

- **Repositórios não estruturados:** Dados geralmente direcionados a usuários finais e que estão guardados em repositórios com menos controles, como compartilhamento em rede, *SharePoint* [6]e estações de trabalho.

É importante que na fase de identificação dos dados sensíveis, a área de Tecnologia da Informação trabalhe juntamente com a de negócios, pois além da identificação, é necessário efetivar as classificações das mesmas e também realizar a combinação de: orientações de processos de negócios, questionários enviados para gestores de negócios, analistas, administrador de banco de dados, desenvolvedores, equipe de *Business Inteligence* (BI), entre outros. Conforme comentado anteriormente, dados sensíveis armazenados em repositórios não estruturados estarão em lugares imprevisíveis, e dado por sua natureza informações importantes estarão incompletas. Devido a isso, o uso de ferramentas como o DLP, conseguem realizar descobertas, através de varreduras em compartilhamento em redes, Intranet, base de dados, servidores e estações de trabalho.

[6] *SharePoint* é uma plataforma onde os colaboradores podem se comunicar, trocar e compartilhar arquivos e trabalharem juntos em um repositório compartilhado (PETERS, 2019).

Estas atividades podem ser praticadas por meio de regras desenhadas para detectar dados sensíveis. As regras são customizadas para cada organização baseada em cada tipo de risco envolvido dos dados identificados. A utilização dessa ferramenta, possibilita o reconhecimento dos repositórios e seus dados para que haja a alteração de local de armazenamento dos dados.

3. Para onde os seus dados estão indo?

As organizações devem entender onde os dados estão indo e como funciona o fluxo de sua movimentação. Esta não é uma tarefa fácil, porém uma gestão bem definida pode auxiliar na transparência do fluxo de transferência dos dados. Se faz necessário o desenvolvimento de uma política de proteção de dados, onde ela terá requisitos específicos para cada tipo de dado classificado e identificado anteriormente. A documentação desta política, deve estar clara a todos os envolvidos, além de incluir alguns tópicos essenciais para a segurança dos mesmos:

- Transferência de dados sensíveis através do *e-mail* e Internet.
- Armazenamento dos dados em estações de trabalho, *notebooks*, dispositivos móveis.
- Uso apropriado das tecnologias de acesso remoto
- O uso de recursos não providos pela organização, como: conta de *e-mail* pessoal, dispositivos móveis e de armazenamento.
- A responsabilidade dos usuários por classificação de documentos que contém dados sensíveis em sua criação.

Adicionalmente, os conceitos da política DLP podem ser usadas na direção da segurança como requisitos no desenvolvimento de projetos, como por exemplo:

- Dados sensíveis não devem ser transmitidos em redes públicas sem criptografia.
- Apenas tecnologias e ferramentas aprovadas pela organização podem ser usadas para troca de informações com terceiros.
- Os acessos a informações sensíveis devem ser registrados e monitorados de forma apropriada
- O acesso a dados armazenados em sistemas informações devem estar restritos apenas aqueles que estão autorizados a acessá-los.

- Dados não podem ser compartilhados com terceiros sem contratos e especificações de requisitos de segurança, onde são obrigados a zelar pela proteção dos mesmos, além da inclusão de monitoração e auditoria por parte da organização na utilização destes dados.

Diante do exposto, vimos de forma abrangente que os dados sensíveis devem ser muito bem avaliados, classificados e que necessita haver uma compreensão de seu fluxo, armazenamento e quais riscos estão envolvidos. O DLP pode ser uma ferramenta muito útil no auxílio de controle e segurança dos dados destes processos apresentados, porém é importante também considerar outros mecanismos para complementar este gerenciamento da segurança de dados. No Quadro 2, Quadro 3 e Quadro 4 será demonstrado os riscos adicionais e outras tecnologias e controles de gerenciamento que podem cooperar com a segurança.

Quadro 2 - Dados em movimento

Área	Exemplo de controle	Tecnologias de suporte
Segurança de perímetro	Prevenção de vazamento de dados	DLP, *firewall*, *proxy server,* IDS/IPS
Monitoramento de rede	Monitoramento de logs e tráfego de rede investigando e identificando transferência de dados inapropriadas	DLP, IDS/IPS
Controle de acesso à Internet	Restrição de uso em acesso a sites não autorizados, upload para nuvem, redes sociais, ferramentas de *backup* online	*Proxy server*, *content filters*
Dados compartilhados com terceiros	Troca de dados com terceiros ocorreu apenas por meios seguros	FTP seguro, mídias físicas encriptadas
Mensageiros instântaneos	Prevenção de transferência de dados com partes externas através de mensageiros instântaneos	*Firewall*, *proxy server*, restrições de uso de aplicativos mensageiros em estações de trabalho

Acesso remoto	Acesso remoto à rede da organização é realizada de forma segura e a existência de controles de dados que podem ser salvos neste acesso remoto em serviços online como *webmail*	Acesso remoto encriptado, restrições para o uso de ferramentas no acesso remoto

Fonte: Ernst & Young (2011)

Quadro 3 - Dados em uso

Área	Exemplo de controle	Tecnologias de suporte
Monitoramento privilegiado de usuário	Monitoramento de ações de usuários privilegiados hábeis para substituir os controles de DLP	Monitoramento de eventos, log de aplicações e operações de base de dados
Monitoramento de acesso/uso	Monitoramento de acesso e uso dos dados sensíveis para identificar potenciais usos inapropriados	Monitoramento de eventos, log de aplicações e operações de base de dados, logs de DLP *endpoint*
Saneamento de dados	Saneamento dos dados sensíveis que não são necessários para uso pretendido	Rotinas de saneamento de dados
Dados usados em testes	Não permitir o uso ou cópia de dados para sistemas que não estão em uso de produção. Saneamento dos dados antes de usá-los nos sistemas de produção	Rotinas de saneamento de dados
Exportação/*save control*	Restringir usuários habilitados a copiar, colar e capturar a tela dos dados sensíveis para utilização em outros locais não aprovados (como *e-mail* por exemplo)	*Endpoint* DLP

Fonte: Ernst & Young (2011)

Quadro 4 - Dados em repouso

Área	Exemplo de controle	Tecnologias de suporte
Endpoint security	Restringir o acesso local para funções de usuários administradores do sistema, prevenindo a instalação, modificação de *softwares* e configurações	Restrições de uso de usuários nas estações de trabalho do sistema operacional. *Endpoint* DLP
Criptografia dos *hosts*	Verificação da encriptação dos discos rígidos dos servidores, estações de trabalho, *notebooks*	Ferramentas de encriptação de discos.
Proteção de dispositivos móveis	Restrição de configurações e habilitar recursos de segurança como senhas	Recursos de segurança incorporados, ferramentas de controle para dispositivos móveis
Rede/Intranet	Gerenciar o acesso à rede e repositórios que possuem dados sensíveis	Controles e restrições de acesso dos sistemas
Controle de mídia física	Prevenção de cópia dos dados para mídias móveis. Verificação para extração de dados que são autorizados apenas de forma encriptada	*Endpoint* DLP, ferramentas de encriptação, restrições de ações das estações de trabalho pelo sistema operacional

Fonte: Ernst & Young (2011)

Assim sendo, para que um programa DLP possa ser efetivo é fundamental entender outros processos de segurança assim como as outras camadas de defesa devem ser implementadas e monitoradas. Como exemplo: mudanças na infraestrutura não que foram cuidadosamente observados e os controles DLP podem se tornar não efetivos, diante disso, é essencial que estes controles de segurança implementados sejam monitorados ao longo do tempo.

Ao se observar as camadas adicionais de segurança, podemos analisar a infraestrutura da empresa com o objetivo de implementar outras soluções, como informadas nas colunas de tecnologia de suporte do Quadro 2, Quadro 3 e Quadro 4. Adiante será apresentado brevemente cada uma delas.

- *Firewall* é uma solução de segurança, sendo na forma de *hardware* ou *software,* que a partir de um conjunto de regras e instruções, realiza a análise do tráfego de rede e determina a partir dessas regras e instruções previamente configuradas, quais ações serão tomadas quanto a transmissão ou recepção dos dados (ALECRIM, 2013).
- *Proxy Server* é uma ponte que conecta o usuário ao restante da Internet. Normalmente quando se é utilizado um navegador para acessar a Internet, uma conexão com o *proxy* é estabelecida, e este recurso redirecionará o usuário com outro lado e a página será exibida. Ao se ter uma solução como essa, é possível controlar e monitorar o uso dos empregados para negar acessos específicos e obter ganho de performance ao guardar uma cópia do *site* localmente, assim, quando houver uma requisição para a mesma página, será carregada de forma mais rápida. Também há a possibilidade de alteração do endereço IP para garantir mais privacidade e a capacidade de encriptação das requisições (PETTERS, 2020).
- *Content Filter* é um recurso de *software* que pode bloquear ou exibir certos conteúdos de páginas da Internet ou *e-mail* que são considerados potencialmente perigosos ou ofensivos. Esta solução é usada em conjunto com *firewalls* e funciona a partir de padrões configurados, como textos ou objetos como imagens que quando carregados em páginas da Internet e coincide com os padrões estabelecidos são barrados (BARRACUDA, 2020).
- *VPN* é a sigla para (*Virtual Private Network*), possibilita ao usuário maior privacidade e anonimato ao criar uma conexão ponta a ponta na rede pública mascarando o endereço IP e encriptando os dados trafegados (SYMANOVICH, 2020).
- IDS sigla que define (*Intrusion Detection Systems*) é uma solução de segurança capaz de analisar, monitorar e sinalizar possíveis ataques a partir de ameaças cibernéticas conhecidas proveniente do tráfego da rede (PETTERS, 2020).
- IPS sigla que define (*Intrusion Prevention Systems)* é uma solução de segurança com características próximas dos *firewalls* onde trabalha

proativamente negando tráfego de rede caso os pacotes trafegados representam ameaças (PETTERS, 2020).

- FTP seguro. Primeiramente precisamos definir que o FTP é a sigla para *File Transfer Protocol*, ou protocolo para transferência de arquivos em português. Com ele, é possível realizar transferência de arquivos, mas sem a inclusão de segurança, pois, os mesmos podem ser trafegados na rede sem criptografia. O FTP seguro nada mais é que incluir criptografia na transferência dos arquivos com propósito de criar confidencialidade dos dados (CONVIANT, 2020).
- Monitoramento de logs. Em um ambiente de rede empresarial, uma grande quantidade de eventos pode ser observada. As ferramentas de segurança como, *firewalls, IDS/IPS*, VPN, roteadores e servidores geram arquivos de *log*[7] que necessitam ser monitorados e analisados constantemente a fim de identificar ameaças e eventos suspeitos quando há mudanças no padrão de funcionamento (REAL PROTECT, 2020).

Um programa estruturado de gerenciamento de riscos focado na perda de dados junto com os controles e gerenciamentos de segurança podem ajudar muito na prevenção de vazamento ou roubo de dados, aditivamente, o modelo conceitual do DLP pode apoiar na construção deste programa tornando-o mais robusto.

Dada a importância do embasamento conceitual do DLP em conjunto a alguns processos úteis para se fazer uma implementação mais assertiva e eficaz da tecnologia, nesta seção será abordado algumas ferramentas, seus recursos e funcionalidades de acordo com as documentações oficiais disponibilizadas gratuitamente pelas empresas, pois, os *softwares* das soluções em si são pagos, e devido a isso, foi optado por um estudo teórico e conceitual expondo as capacidades das soluções nos cenários em que se faz necessário manter uma boa proteção contra possíveis vazamentos de dados.

[7] log *file* é uma extensão de arquivo que é criada automaticamente e onde estão gravados eventos de softwares e de sistema (GAVIN, 2018).

3.1 McAfee Total Protection for Data Loss Prevention

É uma ferramenta de uma das mais conceituadas empresas de *software* de segurança do mundo. A ferramenta DLP da McAfee possibilita a proteção dos dados nos *endpoints*, redes e nuvem de forma rápida e efetiva onde quer que estejam, além de oferecer facilidade de funcionamento para análise dos dados em minutos se adaptando rapidamente à política DLP. Oferece uma interface centralizada para gerenciamento dos incidentes que reduz a complexidade da auditoria, além da visibilidade de todos os dados sensíveis em múltiplos ambientes, auxílio na identificação e dos locais de armazenamento dos dados e classificação deles (MCAFEE, 2019).

Ela também conta com recursos para aplicação de políticas trabalhando com as informações que trafegam em *e-mail*, *gateway*[8]*,* mensageiros instantâneos, assegurando que dados como números de cartões de crédito, dados financeiros ou outras informações que se deseja proteger sejam mantidos com rígida proteção reduzindo os riscos de vazamentos.

No *white paper* (*From Endpoint to Network to Cloud*, 2017) a empresa traz cinco casos de uso em que a ferramenta pode ser efetivamente utilizada abrangendo violações acidentais, roubo de dados por meio acessos privilegiados, *malwares* e pessoas mal intencionadas que trabalham para o negócio.

Primeiro caso: Violação acidental

Este é um caso muito comum e recorrente em qualquer tipo de empresa. Um funcionário com acesso a dados sensíveis pode movê-los para fora da rede da empresa utilizando serviços em nuvem, dispositivos USB ou enviando por *e-mail* com fins de compartilhamento com terceiros, colegas de trabalho e/ou finalizar o trabalho em sua casa. É perceptível que o funcionário não tem intenção maliciosa ao mover as informações, pois elas serão utilizadas no exercício de sua função dentro do negócio, no entanto, do ponto de vista da segurança como já mencionado

[8] *Gateway* é um dispositivo que age como um portão entre duas redes. Ele pode ser um roteador, *firewall*, servidor ou qualquer outro dispositivo capaz de trafegar o fluxo de rede para dentro e fora da rede (TECH TERMS, 2015).

anteriormente, essas ações trazem ameaças colocando riscos de que esses dados possam ser roubados ou vazados. Neste cenário, o DLP da McAfee auxilia bloqueando a ação de transferência das informações rapidamente, e gera um alerta para o time de operações em segurança, assim a política de BYOD e de segurança podem ser aplicadas.

Segundo caso: Vazamento/Roubo de dados do banco de dados

Um outro cenário apresentado, exemplifica um funcionário com privilégio de acesso ao banco de dados e que possui más intenções, possivelmente motivado por vingança, suborno e com intenções de prejudicar financeiramente a empresa, o que categoriza como uma violação grave de política de segurança. O funcionário realiza consultas no banco e tenta enviar os resultados ao um serviço em nuvem. Neste caso, a solução identificaria o destino de envio e faria o bloqueio, geraria um alerta de ação não autorizada, além de aplicar a política de segurança já pré-definida de restrição do *host* ao *firewall.* O analista responsável ao avaliar o incidente em poucos minutos, e teria a possibilidade de retirar o acesso privilegiado do funcionário.

Terceiro caso: Vazamento/Roubo por *Malware* no canal de SSL

Trata de uma situação onde há infecção por *malware* instalado por meio de *phishing* que tem por objetivo explorar um banco de dados. Após a coleta, o *malware* tenta exfiltrar os dados e transmiti-lo através do canal SSL[9]. A McAfee DLP possui função de *Web Gateway* SSL S*canning*, que pode decifrar os dados trafegados na rede com SSL, e que neste caso poderia avaliar se o dado transmitido é sensível ou não para realização de bloqueio. Em menos de um minuto, o DLP alertaria o *firewall* para bloquear o acesso do dispositivo infectado. Após o alerta de incidente, os analistas podem avaliar o caso e providenciar as devidas medidas.

Quarto caso: Vazamento/Roubo via aplicação desconhecida

É um caso sofisticado de ataque, onde uma aplicação confiável instalada, executa funções potencialmente legítimas, mas que contém códigos maliciosos.

---

[9] SSL significa *Secure Sockets Layer*, em resumo, é uma tecnologia para manter uma conexão segura à Internet e resguardar qualquer dado sensível transmitido entre dois sistemas, prevenindo criminosos de ler e modificar qualquer informação (DIGICERT, 2020).

Inicialmente a aplicação teria permissão para acessar os dados sensíveis, porém, com o recurso de inteligência de ameaças, a ação maliciosa poderia ser bloqueada e alertada dentro de segundos ao time de operações de segurança. No *firewall* uma regra de bloqueio seria adotada ao acesso dessa aplicação e a operação de segurança poderia analisar o caso investigando o incidente. O executável dessa aplicação seria enviado a um ambiente isolado para análise de suas funções.

Quinto caso: Empregado mal intencionado

Este cenário engloba um empregado com alto privilégio de acesso e mal intencionado, que tenta driblar a segurança rebaixando a classificação do dado sensível para haver a possibilidade de transferi-lo a um serviço de nuvem ou qualquer outro dispositivo. Neste caso, o funcionário está em uma posição alta na hierarquia da empresa, pois, possivelmente participou da classificação dos dados na implantação do DLP, ou simplesmente tem autorização de gestão para exercer atividades neste setor como: classificar e compartilhar com outros membros do mesmo grupo. A solução da McAfee possibilita que um alerta seja gerado quando o dado for rebaixado em sua classificação e bloqueia a operação de transferência.

3.2 Teramind DLP

A Teramind foi fundada em 2014, com sua sede em Miami, Flórida. Fornece serviços em escala global de monitoramento de empregados, análise de comportamento de usuário, detecção de ameaças internas (*insiders*), forense computacional e soluções de prevenção de perda de dados (TERAMIND, 2020).

A solução DLP oferecida pela empresa Teramind, disponibiliza o recurso de a análise de comportamento inteligente, ajudando a identificar intenções suspeitas, erros e acidentes que resultariam em brechas de segurança ou tentativas de exfiltração de dados. Uma outra função da ferramenta são os recursos de gerenciamento de conformidade, auxiliando em normas como: GDPR, HIPAA, PCI DSS e ISO 27001. Tem como público alvo pequenos e médios negócios e empresas do setor público (TERAMIND, 2020).

A Teramind (2020) disponibiliza 3 tipos principais de implantações flexíveis, e mais alguns recursos utilizados dentro da ferramenta, que são:

***On-premise*:** É definida pelos seguintes pontos: fácil implementação, controle total do seu ambiente, armazenamento e rotina de *backups*. A implementação da ferramenta será inteiramente controlada pela empresa que contratou, não dependendo de serviços de *cloud*. É recomendado para empresas que precisam de mais controle em seus ambientes ou possuem políticas de *compliance* rígidas. As especificações para esse método de implementação são:

- *Appliance* virtual roda em *VMWare*, *Hyper-V* ou *XenServer*;
- Necessário aproximadamente 1GB de armazenamento por 160 horas de dados e captura de tela com alta qualidade;
- Mínimo de 10kbps *upstream* (*agent to server*, depende também da atividade dos usuários).

***Private Cloud*:** A implementação da ferramenta poderá ser feita em um serviço de cloud de confiança da empresa. Utilizando a AWS como exemplo, as principais vantagens desta implementação são: seu preço flexível pagando apenas pelos recursos consumidos, possibilidade da customização e escalabilidade do ambiente, caso haja a demanda, alta disponibilidade, redundância e *backup* e recuperação de desastres por demanda.

Teramind *Cloud*: O gerenciamento da implementação da ferramenta e da infraestrutura será feito pela própria Teramind, restando apenas que a empresa instale o Teramind *Agent* nas máquinas que serão monitoradas e configurar os usuários, políticas e regras que serão aplicadas. As vantagens desta implementação são: realização automática de *backups*, sem necessidade de manutenção, todas as comunicações utilizarão SSL e fácil integração com um *Active Directory* já existente.

Recursos da ferramenta

Observação em tempo real e de gravações passadas: É feita a gravação de todas as ações que o usuário fez no dispositivo em determinado período, permitindo a visualização da tela ao vivo e do histórico de conteúdo acessado. Suas principais características são:

- *Streaming* em tempo real da atividade de usuários através do painel da ferramenta.

- Gravação das atividades dos usuários fica disponível para ser acessado e visualizado pelo administrador.
- Todas as atividades são monitoradas e gravadas, desde o pressionar das teclas até ações tomadas dentro de aplicações.
- Registros extensos permitem a consulta de gravações.
- Os arquivos gravados podem ser exportados em formato “.avi”.

Monitoramento de websites: Possibilita o monitoramento da atividade online dos empregados, com o objetivo de analisar a produtividade deles. Tem como principais características:

- URLs e *websites* que foram digitados são acrescentados em um registro em texto do usuário, que é complementado com uma gravação do ocorrido, que também inclui as atividades realizadas nestes sites.
- Alertas podem ser configurados para avisar ao usuário sobre o tempo que ele passou ocioso, se está sendo feito o *upload* ou *download* indevido de arquivos sensíveis ou ao acessar sites de entretenimento, ou que foram determinados pelo gestor da ferramenta como indevidos.

Monitoramento de *e-mail*: No envio ou no recebimento de *e-mails*, a ferramenta DLP grava todas as informações referentes a ação tomada, sendo um componente essencial para a identificação de ameaças internas e na prevenção a perda de dados. Suas características são:

- Todos os eventos associados ao envio e recebimento de *e-mails*, desde o conteúdo que foi lido/escrito até documentos anexados são gravados para consulta posterior.
- Possui suporte a todas as plataformas de *e-mail* (exemplos são: *Outlook*, *Gmail*, *Yahoo*, Yandex e outros).
- Alertas podem ser configurados caso *e-mails* sejam enviados para contas não corporativas.

Registro do pressionamento de teclas: Captura toda atividade do teclado, e toda tecla individual pressionada e ações de copiar/colar, gravando toda a informação em registros, sejam de empregados que trabalham em regime *on-site* ou remotamente. As principais características desta função são:

- Criação de evidências visuais e textuais das teclas pressionadas e ações como copiar/colar;
- Criação de regras que impedem a criação de registros sensíveis, como informações bancárias;
- É feito o registro de caracteres invisíveis e ocultos.

Monitoramento de arquivos: Possibilita o monitoramento de todas as atividades envolvendo arquivos, como criação, exclusão, acessos e modificações. Essa função pode ser acompanhada das seguintes ações:

- Notificação quando for feito o *upload* de arquivos ou utilizados como anexo de *e-mail*.
- Bloqueio dos privilégios de leitura e escrita em pastas de dispositivos USB.
- Prevenção do acesso não autorizado a arquivos específicos.
- Rastreamento dos “movimentos” dos arquivos pelo sistema, mesmo que tenha sido aberto ou alterado em programas de terceiros.

Rastreamento de documentos impressos: A ferramenta DLP coleta todas as requisições de impressão de documentos que é feita por usuários e administradores, gravando a informação. Podem ser vistos os conteúdos do documento que seria impresso e configurados alarmes para avisar quando forem requisitadas impressões de informações sensíveis.

Reconhecimento Ótico de Caracteres: Permite a descoberta de PII[10], PHI[11] e PFI[12] e outras informações sensíveis que estejam a mostra na tela. Oferece a busca por informações textuais em imagens e vídeos, facilitando uma possível investigação forense.

---

[10] PII: *Personally Identifiable Information*, ou Informações Pessoais Identificativas. Informação que possibilita a terceiros identificarem quem você é (CYNTELL, 2020).

[11] PHI: *Personal Health Information*, ou Informações Pessoais de Saúde. Informação que pode revelar diagnósticos, doenças e tratamentos seus (CYNTELL, 2020).

[12] PFI: *Personal Financial Information*, ou Informações Financeiras Pessoais. Informação que pode te identificar e prover informações sobre seus investimentos, situação de crédito, empréstimos, entre outras informações (CYNTELL, 2020).

Regras inteligentes e alertas automatizados: Possibilita a configuração de regras para notificar, bloquear, redirecionar ou realizar o *logout* dependendo da severidade da ofensa realizada pelo usuário.

Análise de produtividade do empregado: É feita a coleta de numerosos dados para criar um relatório rico em informações sobre as funções e produtividade dos usuários.

Monitoramento de aplicações: Registra toda atividade que ocorre em cada aplicação rodando no dispositivo, mantendo gravações da aplicação e registros em texto que são atualizadas a cada segundo que o usuário gasta utilizando a aplicação.

Monitoramento da rede: Permite o monitoramento o tráfego da rede, incluindo todas as aplicações e usuários conectados à Internet, exibindo horário e portas utilizadas na conexão. Os relatórios completos, disponíveis para o administrador da rede, mensuram a largura de banda utilizada por cada empregado individual e os respectivos computadores utilizados para estabelecer a conexão.

Monitoramento de mensageiros instantâneos: Possibilita o monitoramento, formas de reação a conversas, como bloquear o *chat* que tenham como conteúdo palavras-chave inapropriadas, e registra todo o conteúdo capturado.

Monitoramento de redes sociais: Viabiliza o monitoramento e formas de reação ao uso de redes sociais por empregados, podendo restringir ou bloquear o acesso a sites e aplicativos de redes sociais, alertar usuários sobre tempo gasto nas mesmas e registrar todas as informações de interações ocorridas (data e hora, empregado, dispositivo de origem, mensagens, anexos e ações realizadas).

Controle remoto da área de trabalho: Permite a sobreposição de comandos enviados ao dispositivo, fazendo com que o empregado perca o controle manual do mesmo.

Analíticas de Comportamento de Usuários e Entidades: Identifica e alerta ao administrador possíveis ameaças e comportamentos anômalos seguindo uma base comportamental.

3.3 Endpoint Protector DLP

Em seu documento oficial (*Industry-Leading Data Loss Prevention* (DLP)) a DLP *Endpoint Protector* informa que a solução é projetada para trabalhar na proteção de dados confidenciais contra agentes internos mal intencionados enquanto possibilita manter o negócio com maior produtividade, conveniência, de forma agradável e segura. A solução é ideal para empresas que possuem em seu ambiente de produção diversos sistemas operacionais (*Windows,* Mac, Linux) e redes interligados. É citado seis dos principais benefícios oferecidos nesta solução.

Facilidade de instalação de gerenciamento: *Endpoint Protector* pode ser instalado, configurado e estar em funcionamento dentro de 30 minutos.

Perfis de conformidade predefinidos: Possui políticas pré-definidas fáceis de implementação que estão em conformidade com a (GDPR, HIPAA, PCI DSS).

Proteção multiplataforma: A solução oferece recursos e alto nível de proteção para plataformas que utilizam sistemas *Windows*, Mac e Linux.

Relatórios detalhados de atividades de usuários: *Endpoint Protector* permite rastrear e reportar atividades de dados sensíveis.

Flexibilidade de opções: É oferecido diversas formas de implementações que se adaptam facilmente à infraestrutura e necessidade do negócio.

Políticas granulares: Facilidade na implantação de segurança de usuários e grupos para acesso de dispositivos removíveis.

Um dos recursos mais interessantes desta solução, é a variedade do tipo de implementação, permitindo uma maior flexibilidade ao cliente, facilitação de implantação e gerenciamento. Elas estão divididas em três categorias.

- *Cloud Services* é um tipo de implementação onde a solução será instalada e configurada em um servidor provedor de serviços em nuvem como AWS, GCP ou Microsoft Azure. Após o recebimento da solução, rapidamente é possível instalar e configurar em um dos serviços de nuvem mencionados anteriormente, de maneira rápida e eficiente (ENDPOINT PROTECTOR, 2020).

- *Virtual Appliance* é uma implementação que funciona com ambiente virtual, compatível com os principais *softwares* de virtualização (*VirtualBox, VMware Parallels, Microsoft Hyper-V*). A instalação no ambiente virtual é rápida, onde é possível importar os clientes *Endpoint Protector* instalados nos dispositivos. Possui diversos benefícios como: escalabilidade com número exato de licença dos dispositivos móveis que quer proteger, fácil aprendizado com utilização de uma interface *web,* todos os módulos inclusos (encriptação, controle de dispositivos, proteção de conteúdo, MDM, controle de conteúdo) (ENDPOINT PROTECTOR, 2020).
- *Hardware Appliance* é uma categoria em que é possível adquirir um dispositivo físico que inclui todos recursos já instalados, bastando apenas alimentar com energia e incluí-lo na rede local associando um endereço de IP. Existem diversas modelos que se adaptam ao tamanho da organização, sendo que o mais básico consegue proteger 50 computadores, e o mais sofisticado 4000 computadores. Seus benefícios incluem: *Hardware* dedicado*,* redução de tempo com configurações, interface *web* de fácil gerenciamento (ENDPOINT PROTECTOR, 2020).

O *Endpoint Protector* trabalha com basicamente quatro funções para a mitigação de perda de dados, que são: *Device Control, Content-Aware Protection, Enforce Encryption.*

- ***Device Control:*** É a solução mais granular do mercado permitindo controle de dispositivos USB e de armazenamento. Ele é a primeira camada de segurança provida pelo *Endpoint Protector*. Através da interface é possível gerenciar todos os dispositivos USB e portas periféricas dos computadores (ENDPOINT PROTECTOR, 2020).

  A função *Device Control* trabalha com alguns recursos úteis para gerenciamento de dispositivos USB como: estabelecimento de permissões por (dispositivos, usuário, máquinas e grupos), permissões de acesso por (aceitação e negação, somente leitura), alertas (conectado e desconectado), controles de dispositivos e portas mais comuns (dispositivos USB, discos externos, *smartphones, tablets*, *players* de áudio e vídeo, cartões de memória, impressoras, dispositivos *wireless*, *bluetooth*¸ teclados). Adicionalmente,

proporciona o envio de logs para um servidor central e força a encriptação dos dados transferidos quando estes dispositivos estão autorizados pela ferramenta (ENDPOINT PROTECTOR, 2020).

- ***Content-Aware:*** Com o crescimento da disponibilidade e utilização de serviços em nuvem e *webmail* trouxe consigo mais causas de incidentes envolvendo vazamentos de dados acidentais e não intencionais. Com o *Content-Aware* é possível mitigar esses problemas protegendo as informações sensíveis. Esta solução oferece uma maneira avançada de inspecionar dados, incluindo imagens (.jpeg, .png, .gif, .bmp, .tiff), arquivos de escritório (.docx, .pptx, .xlsx, .pstx, .pdf), arquivos compactados (.zip .rar .ace .tar), programas (.ccp .java .py .sh, .csh .bat,), executáveis (.exe), mídias (.mp3 .mp4 .m4a .avi, .wma). É possível também aplicar em contexto de aplicações como: *e-mail (Outlook)*, *browsers (Firefox, Internet Explorer, Google Chrome, Safari)*, mensageiros instantâneos (Skype, *Yahoo Messenger*), serviços de nuvem (*Dropbox, ICloud,* BitTorrent) (ENPOINT PROTECTOR, 2020).
- ***Enforced Encryption*** esta solução de encriptação possibilita uma maneira de garantir confidencialidade de dados para que não caiam em mãos erradas. Com o *EasyLock* USB *Enforced Encryption* combinados ao *Endpoint Protector* permite aos administradores estender as políticas de controle de dispositivos, certifica que os dados transferidos a um dispositivo USB de armazenamento seja automaticamente encriptado. É compatível com múltiplas plataformas (*Windows*, Mac, Linux, IOS, *Android*), possui a vantagem de controle em um mesmo console de administração (ENPOINT PROTECTOR, 2020).

Após o estudo dos recursos e funcionalidades das ferramentas DLP, foi possível compreender de forma abrangente suas capacidades, utilidades e como podem ser utilizadas para mitigação de perda ou vazamento de dados em possíveis cenários e situações comuns do dia a dia das empresas. A seguir, para fins de conclusão deste estudo, apresentaremos no Quadro 5 as principais ameaças que foram apresentadas anteriormente neste presente trabalho, comparando cada uma das soluções e o que cada uma delas oferece como mitigação.

Quadro 5 - Comparativo de soluções DLP

	Ferramentas Abordadas		
Ameaças/Vulnerabilidades	**McAfee DLP**	**Teramind DLP**	**Endpoint Protector DLP**
Utilização de *notebook* em redes inseguras	✔	**?**	✔
Perda/Roubo do dispositivo	**?**	**?**	✔
Bugs de software	✔	**?**	✔
Bugs de aplicativos	✔	**?**	✔
Aplicativos maliciosos	✔	✔	✔
Rooting/Jailbreaking	**?**	**?**	**?**
Acesso indevido a informações	✔	✔	✔
Phishing	✔	✔	**?**
Ataques direcionados e vulnerabilidades	**?**	**?**	✔
Transferência não segura de dados	✔	✔	✔
Uso de dispositivos moveis em redes não confiáveis/seguras	**?**	**?**	**?**
Acesso a conteúdo não confiável	✔	✔	✔

Fonte: Autoria própria

Legenda: ✔ - Oferece proteção; **?** - Não informado na documentação.

Considerações finais

No decorrer deste estudo, foi possível compreender os riscos de roubo e/ou vazamento de dados em um ambiente empresarial perante a prática do BYOD, visto que, a informação é um ativo valioso responsável por fazer os processos de negócios funcionarem. As constantes mudanças e novidades tecnológicas alteram a forma como as relações entres as pessoas ocorrem, e também afetam diretamente o modo como elas lidam no exercício do seu trabalho, de maneira que, a prática do BYOD foi uma consequência desse fato, logo, surgiu uma nova questão do ponto de vista da Segurança da Informação, em como aderir essa nova realidade minimizando os riscos.

Diante disso, foi dada a importância neste tema com o objetivo elencar algumas soluções de segurança na implantação do BYOD com o DLP, buscando contribuir com a mitigação de riscos em diferentes organizações. Vale ressaltar a importância em também estabelecer outros controles tecnológicos como as soluções de *firewall*, IDS/IPS, *proxy server*, MDM, ESS e controles de gestão como, políticas de Segurança da Informação e políticas BYOD a fim de mitigar possíveis ameaças aos dados sensíveis, deste modo, o objetivo foi alcançado.

Dado o aprofundamento no estudo de controles tecnológicos, sobretudo o DLP junto com o processo de gestão e análise dos dados para implantação desta solução, inferimos que é uma adoção conveniente para atenuar as ameaças de incidentes de Segurança da Informação. A escolha pela ênfase no DLP, ocorreu no estudo e percepção da eficácia da união dos recursos e funcionalidades integrados a este tipo de tecnologia.

Por conseguinte, o trabalho partiu da hipótese de que a adoção do DLP combinado aos demais controles e tecnologias, possibilita a construção de uma infraestrutura robusta e mais segura, assim, todos estes controles bem configurados e geridos corretamente conseguem mitigar muitos problemas no âmbito da segurança de dados. Durante o estudo, verificou-se as principais ameaças associadas ao BYOD e como contorná-las a partir da adoção de procedimentos e ferramentas que auxiliam a fechar brechas. Estas análises estão presentes no capítulo 3, Quadro 1, Quadro 2, Quadro 3, Quadro 4 e Quadro 5, deste modo, a hipótese foi confirmada.

As pesquisas seguiram na busca por informações e dados, de artigos, notícias e documentações de empresas conceituadas que abordam o tema. As informações abrangem dados estatísticos, casos cotidianos, estudos e análises realizados por especialistas, com intuito de confirmar que os riscos abordados estão realmente presentes no dia a dia das empresas.

A princípio, seria feito uma prova de conceito das ferramentas citadas neste trabalho, utilizando um simulador de rede; máquinas virtuais interligadas com sistemas operacionais *Windows,* Linux, *Android* (emulado); *firewall*; *proxy server* e uma solução DLP, todavia, devido às limitações financeiras, não foi possível prosseguir, porque até então as soluções de *Data Loss Prevention*, que ainda possuem suporte, são proprietárias e pagas, bem como disponibilizadas para teste com utilização limitada de funcionalidades e de dias. Como resultado, foi somente praticável efetivar o estudo teórico a partir das documentações oficiais disponíveis nos sites das próprias soluções, onde é possível entender de forma abrangente as capacidades dessas soluções, mas sem muita minúcia dos fatos observados, assim, foi feito a comparação das principais ameaças trazidas pelo BYOD e como algumas opções de DLP poderiam auxiliar na mitigação.

Por fim, o presente estudo demonstrou como a adoção de algumas soluções de Segurança da Informação, com ênfase no DLP, podem ser úteis na proteção dos dados sensíveis das empresas. Algumas delas já conhecidas e utilizadas, outras mais recentes e que estão aos poucos adentrando no mercado. Uma recomendação para prosseguimento da pesquisa é a aplicação de uma infraestrutura de rede corporativa simulada através de softwares, realizando análises e provas de conceito de uma solução DLP disponível para teste gratuito, e dos demais controles de segurança.

Referências

AARON, M. French; CHENGQI, John Guo; J.P.Shim. COMMUNICATIONS OF THE ASSOCIATION FOR INFORMATION SYSTEMS. **Current Status, Issues, and Future of Bring Your Own Device (BYOD)**, 2014. Disponível em <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3819&context=cais> Acesso em 28 de set de 2019.

ALECRIM, Emerson. **O que é firewall?** – Conceito, tipos e arquiteturas, 2013. Disponível em <https://www.infowester.com/firewall.php> Acesso em: 9 de jun de 2020.

AVAST. **O que é malware?** 2020. Disponível em: <https://www.avast.com/pt-br/c-malware> Acesso em 07 de jun de 2020.

BARRACUDA. **Content filtering**. Disponível em <https://www.barracuda.com/glossary/content-filtering> Acesso em 9 de jun de 2020.

BELCIC, Ivan. **What is a proxy server?** 2020 Disponível em <https://www.avast.com/c-what-is-a-proxy-server> Acesso em 9 de jun de 2020.

BERNHARDT, Melody. **BYOD:** How your business can address the 5 biggest vulnerabilities, Disponível em: <https://ccbtechnology.com/byod-5-biggest-security-risks/>. Acesso em: 04 de mar de 2020.

BILIC´, Denise. **Mitos sobre a segurança móvel**, #2: o rooting ou jailbreaking não afetam a proteção, 2016. Disponível em <https://www.welivesecurity.com/br/2016/11/08/mitos-rooting-jailbreaking/> Acesso em: 7 de jun de 2020.

BISCOM. **Employee Departure Creates Gaping Security Hole, Says New Data**, 2015. Disponível em: <https://www.biscom.com/employee-departurecreates-gaping-security-hole-says-new-data/> Acesso em: 08 de nov de 2019.

BOXALL, Andy. **Malware alert:** If you downloaded these 3 Android apps, remove them immediately. Disponível em: <https://www.digitaltrends.com/mobile/googleremoves-adware-app-from-google-play/>. Acesso em 19 de out de 2019.

BRADLEY, Joseph. **New Analysis:** Comprehensive BYOD Implementation Increases Productivity, Decreases Costs, 2013. Disponível em<https://blogs.cisco.com/news/new-analysis-comprehensive-byod-implementation-increases-productivity-decreases-costs> Acesso em 21 de set de 2019.

BURNHAM, Jennifer Deming. **The Rise and Risk of BYOD**, 2014. Disponível em: <https://www.druva.com/blog/the-rise-and-risk-of-byod/#.U3uwoNxU5-A>. Acesso em: 04 de mar de 2020.

CALERO. **BYOD VS. CYOD VS. COPE** – How to choose the right enterprise mobility strategy, 2019. Disponível em: <https://www.calero.com/mobility-service-

support/byod-vs-cyod-vs-cope-choose-right-enterprise-mobility-strategy/>. Acesso em: 24 de fev de 2020.

COMPTIA. **CompTIA Study Reveals Mobility Push Continues, but New Challenges Lie Ahead for Many U.S Companies**, 2014. Disponível em: <https://pt.slideshare.net/comptia/slideshare-charts-2014-mobility-study> Acesso em 9 de set de 2019.

CONVIANT, software. **What is Secure FTP?** Disponível em <https://www.coviantsoftware.com/technology-briefs/what-is-secure-ftp/> Acesso em 11 de jun de 2020.

CYNTELL. **Privacy versus Security**, Disponível em: <https://cyntell.com/privacy-versus-security/> Acesso em: 17 de jun de 2020.

DIGICERT **What is an SSL Certificate**. Disponível em <https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https> Acesso em: 19 de jun de 2020.

DUY, Dang-Pham. **Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university:** A Protection Motivation Theory approach, 2015. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404814001643>. Acesso em: 4 de nov de 2019.

ENDPOINT PROTECTOR. **100% Deployment Flexibility & Fast Setup**. Disponível em: <https://www.endpointprotector.com/solutions/content-aware-data-loss-prevention> Acesso em 16 de jun de 2020.

ENDPOINT PROTECTOR **Content-Aware Data Loss Prevention**. Disponível em: <https://www.endpointprotector.com/products/endpoint-protector/appliance> Acesso em 16 de jun de 2020.

ENDPOINT PROTECTOR. **Enpoint Protector Device Control**. Disponível em: <https://www.endpointprotector.com/solutions/device-control> Acesso em 16 de jun de 2020.

ENDPOINT PROTECTOR. **Enforced Encryption**. Disponível em: <https://www.endpointprotector.com/solutions/enforced-encryption> Acesso em 16 de jun de 2020.

ENDPOINT PROTECTOR. **Industry-Leading Data Loss Prevention (DLP)**, 2019. Disponível em: <https://www.endpointprotector.com/support/pdf/datasheet/Data_Sheet_Endpoint_Protector_5_CoSoSys_EN.pdf> Acesso em 16 de jun de 2020.

ERNST & YOUNG. **Bring your own device. Security and risk considerations for your mobile device program**, 2013. Disponível em: <https://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf>. Acesso em: 2 de set de 2019.

ERNST & YOUNG. **Data loss prevention**: Keeping your sensitive data out of the public domain, 2011. Disponível em: <https://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf>. Acesso em: 8 de fev de 2020.

ERNST & YOUNG. **The dangers of BYOD:** How can you protect your organization? 2017. Disponível em <https://consulting.ey.com/the-dangers-ofbyod-how-can-you-protect-your-organization/>. Acesso em 9 de set de 2019.

FORCEPOINT. **What is Bring Your Own Device (BYOD)?** 2019. Disponível em: <https://www.forcepoint.com/cyber-edu/bring-your-own-device-byod>. Acesso em: 10 de set de 2019.

GAVIN, Brady. **What is a Log File (and How Do I Open One)?** 2018. Disponível em <https://www.howtogeek.com/359463/what-is-a-log-file/> Acesso em 11 de jun de 2020

HAMBLEN, Matt. **The bring-your-own-device fad is fading**: CompTIA survey finds 53% of private companies ban BYOD, 2015. Disponível em: <https://www.computerworld.com/article/2948470/the-bring-your-own-device-fad-is-fading.html> Acesso em 2 de set 2019.

HOCKLY, Nicky. **Tech-savvy teaching:** BYOD, 2012. Disponível em <https://itdi.pro/itdihome/advanced_courses_readings/Hockly_MET-21.4libre.pdf>. Acesso em 30 de set de 2019.

HOELSHCER, Penny. **BYOD security:** What are the risks and how can they be mitigated? 2017. Disponível em <https://www.comparitech.com/blog/information-security/byod-security-risks/> Acessem em 12 de out de 2019.

HUGHES, Neil. **Despite security risks of free public Wi-Fi, 81% still connect to it, OWI Labs survey finds –** One World Identity, Disponível em: <https://oneworldidentity.com/despite-security-risks-free-public-wi-fi-81-percent-still-connect-owi-labs-survey-finds/>. Acesso em: 04 de mar de 2020.

IBOPE Conecta. **Pesquisa IBOPE CONECTA:** 48% das micro e pequenas empresas brasileiras planejam comprar computadores em até seis meses, 2017. Disponível em: <https://www.dell.com/learn/br/pt/en/press-releases/2017-06-05-ibope-conecta-survey> Acesso em 2 de set de 2019.

IBM Services. **BYOD balance**: Bring your own device can be productive and secure, 2019. Disponível em: <https://www.ibm.com/services/digitalworplace/byod>. Acesso em: 4 de nov em 2019.

INTEL. **Insights on the Current State of BYOD**, 2012. Disponível em: <https://www.intel.com/content/dam/www/public/us/en/documents/whitepapers/consumerization-enterprise-byod-peer-research-paper.pdf>. Acesso em: 3 de out de 2019.

KASPERSKY. **O que são exploits e por que são tão temidos?** 2016. Disponível em: <https://www.kaspersky.com.br/blog/exploits-problem-explanation/6010/> Acesso em 7 de jun de 2020.

KEEPER. **How to Provision Employees in a BYOD World**, 2016. Disponível em: <https://keepersecurity.com/assets/pdf/Keeper-White-Paper-How-toProvision-Employees-in-a-BYOD-World.pdf>. Acesso em: 14 de out de 2019.

KEYES, Jessica. **BYOD:** Mobile Device Threats and Vulnerabilities, Disponível em: <http://www.ittoday.info/ITPerformanceImprovement/Articles/2014-07Keyes2.html>. Acesso em: 04 de mar de 2020.

KINGSLEY-HUGHES, Adrian. **6 Threats Facing BYOD**, Disponível em: <https://www.zdnet.com/article/6-threats-facing-byod/>. Acesso em: 04 de mar de 2020.

LOVE, Dylan. **The Latest Jailbreak Statistics Are Jaw-Dropping**, Disponível em: <https://www.businessinsider.com/jailbreak-statistics-2013-3>. Acesso em: 04 de mar de 2020.

LUCIDCHART. **Solving the challenges of an Envolving Workplace**, 2019. Disponível em: <https://www.lucidchart.com/pages/research/2019-it-report>. Acesso em 3 de nov de 2019.

MCAFEE. **BYOD Endpoint Security**. Disponível em: <https://www.mcafee.com/enterprise/pt-br/security-awareness/endpoint/byod-endpoint-security.html>. Acesso em: 04 de mar de 2020.

MCAFEE. **From Endpoint to Network to Cloud**, 2017. Disponível em: <https://www.mcafee.com/enterprise/en-us/assets/white-papers/restricted/wpendpoint-network-cloud-pervasive-threats.pdf>. Acesso em: 10 de nov de 2019.

MCAFEE **Total Protection for Data Loss Prevention**. Lock down you data, not your business. Solution Brief, 2019. Disponível em: <https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-total-protection-for-dlp.pdf.> Acesso em: 27 de mai de 2020.

MARK A. HARRIS, ELIZABETH REGAN, KAREN PATTEN. **The Need for BYOD Mobile Device Security Awareness and Training**, 2013. Disponível em: <https://www.researchgate.net/profile/Mark_Harris29/publication/289304384_The_need_for_BYOD_mobile_device_security_awareness_and_training/links/56d6e45608aebe4638aefd7a/The-need-for-BYOD-mobile-device-securityawareness-and-training.pdf.>. Acesso em: 4 de nov de 2019.

MYCYBERSECURITY. **Antimalware**. Disponível em: <https://www.mycybersecurity.com.br/glossario/antimalware/> Acesso em: 7 de jun de 2020.

NTTSECURITY. **Endpoint Security Services (ESS)**. Disponível em: <https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl_solution_overview_ess_uea> Acesso em: 7 de jun de 2020.

NUSCA, Andrew. **BYOD:** North America and Asia embrace it Western Europe not so much, 2013. Disponível em: <https://www.zdnet.com/article/byod-northamerica-and-asia-embrace-it-western-europe-not-so-much/>. Acesso em: 1 de out de 2019.

OKYLE, Carly. **Why your password is Hackerbait (Inforgraphic)**, 2015. Disponível em: <https://www.entrepreneur.com/article/242208>. Acesso em: 19 de out de 2019.

OPSITNICK, Timothy; ANGUILANO, Joseph; TUCKER, Trevor. **Using Computer Forensics to Investigate Employee Data Theft.** Disponivel em: <https://www.tcdi.com/computer-forensics-whitepaper-trevor-tucker-joe-anguilano-tim-opsitnick/> Acesso em 08 de nov de 2019.

PALOALTO **What is an Endpoint?** Disponível < https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint> Acesso em 11 de jun de 2020.

PETERS, Aaron. **What is SharePoint and What Dows It Do?** 2019. Disponível <https://www.lifewire.com/what-is-sharepoint-4176266> Acesso em 20 de jun de 2020.

PETTERS, Jeff. **IDS vs. IPS:** What is the Difference? <https://www.varonis.com/blog/ids-vs-ips/> Acesso em 11 de jun de 2020.

PETTERS, Jeff. **What is a proxy server and how does it work?** <https://www.varonis.com/blog/what-is-a-proxy-server/> Acesso em: 9 de jun de 2020.

PREY. **Mobile Theft and Loss Report**, Disponível em: <https://preyproject.com/uploads/2019/02/Mobile-Theft-Loss-Report-2018.pdf>. Acesso em: 04 de mar de 2020.

QING, Liau Yun. **BYOD on rise in Asia, but challenges remain**, 2013. Disponível em <http://zdnet.com/article/byod-on-rise-in-asia-but-challengesremain/>. Acesso em 1 de out de 2019.

REAL PROTECT. **Monitoramento de Logs.** Disponível em: <https://realprotect.net/monitoramento-de-log/ > Acesso em 11 de jun de 2020.

ROUSE, Margaret. **Mobile Device Managegement (MDM)**, 2020. Disponível em: <https://searchmobilecomputing.techtarget.com/definition/mobile-device-management> Acesso em 7 de jun de 2020.

SANDERS, Andrew. **15 (CRAZY) Malware and Virus Statistics, Trends and Facts 2020**, Disponível em: <https://www.safetydetectives.com/blog/malware-statistics/>. Acesso em: 04 de mar de 2020.

SÊMOLA, Marcos. **GESTÂO DA SEGURANÇA DA INFORMAÇÃO:** uma visão executiva. 2 ed. Rio de Janeiro: Elsevier, 2003.

STEPHEN, Gandel. **Lloyd's CEO:** Cyber atack costs companies $400 bilion every year, 2015. Disponível em: <https://fortune.com/2015/01/23/cyber-attackinsurance-lloyds/>. Acesso em: 16 de out de 2019.

SYMANOVICH, Steve **What is a VPN?** Disponível em: <https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html> Acesso em 11 de jun de 2020.

TECH TERMS. **Gateway**, 2015. Disponível em <https://techterms.com/definition/gateway> Acesso em 11 de jun de 2020.

TERAMIND. **On-Premise Deployment**, Disponível em: <https://www.teramind.co/product/deployment/on-premise> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Application Monitoring**, Disponível em: <https://www.teramind.co/features/application-monitoring> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind - Dashboard**, Disponível em: <https://democompany.teramind.co> Acesso em: 12 de jun de 2020.

TERAMIND. **Teramind – Email Monitoring**, Disponível em: <https://www.teramind.co/features/email-monitoring> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Employee Productivity Analysis**, Disponível em: <https://www.teramind.co/features/productivity-analysis> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – File Transfer Tracking**, Disponível em: <https://www.teramind.co/features/file-transfer-tracking> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Instant Message Monitoring**, Disponível em: <https://www.teramind.co/features/instant-message-monitoring> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Keystroke Logger**, Disponível em: <https://www.teramind.co/features/keystroke-recorder-logger> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Live View & History Playback**, Disponível em: <https://www.teramind.co/features/live-desktop-view-history-playback> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Network Monitoring**, Disponível em: <https://www.teramind.co/features/network-monitoring> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Optical Character Recognition (OCR)**, Disponível em: <https://www.teramind.co/features/ocr-optical-character-recognition> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Printed Document Tracking**, Disponível em: <https://www.teramind.co/features/printed-document-tracking> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Remote Desktop Control**, Disponível em: <https://www.teramind.co/features/remote-desktop-control> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Smart Rules & Automated Alerts**, Disponível em: <https://www.teramind.co/features/smart-rules-automated-alerts> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Social Media Monitoring**, Disponível em: <https://www.teramind.co/features/social-media-monitoring> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – User & Entity Behavior Analytics (UEBA)**, Disponível em: <https://www.teramind.co/features/ueba-user-and-entity-behavior-analytics> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind – Website Monitoring**, Disponível em: <https://www.teramind.co/features/internet-use-monitoring> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind Cloud Deployment Solution**, Disponível em: <https://www.teramind.co/product/deployment/cloud> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind DLP - Effective Endpoint Data Loss Prevention Solutions**, Disponível em: <https://www.teramind.co/product/dlp-data-loss-prevention> Acesso em: 12 de jun de 2020.

TERAMIND. **Teramind on AWS – Deployment Guide**, Disponível em: <https://www.teramind.co/images/cms/Teramind-AWS-deployment-guide-v5-2019-08-12.pdf> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind on AWS**, Disponível em: <https://www.teramind.co/deployment/aws> Acesso em: 17 de jun de 2020.

TERAMIND. **Teramind On-Premise – Deployment Guide**, Disponível em: <https://www.teramind.co/images/cms/Teramind-On-Premise-Deployment-Guide-2020-03-13.pdf> Acesso em: 17 de jun de 2020.

TELWARE. **Three Major BYOD Security Vulnerabilities**, Disponível em: <https://www.telware.com/news/three-major-byod-security-vulnerabilities>. Acesso em: 04 de mar de 2020.

TRENDMICRO. **Infosec Guide:** Dealing with Threats to a Bring Your Own Device (BYOD) Environment, Disponível em: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-infosec-guide-bring-your-own-device-byod>. Acesso em: 04 de mar de 2020.

VERIZON. **2017 Data Breach Investigations Report**, Disponível em: <https://enterprise.verizon.com/resources/reports/2017_dbir.pdf>. Acesso em: 04 de mar de 2020.