ANÁLISE COMPARATIVA DE FERRAMENTAS DE GERENCIAMENTO DE CONTEÚDO VISANDO O COMPARTILHAMENTO SEGURO DE INFORMAÇÕES CORPORATIVAS

CARLO ALESSANDRO MELO NOCE

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ANÁLISE COMPARATIVA DE FERRAMENTAS DE GERENCIAMENTO DE CONTEÚDO VISANDO O COMPARTILHAMENTO SEGURO DE INFORMAÇÕES CORPORATIVAS

CARLO ALESSANDRO MELO NOCE

ORIENTADOR: GEORGES DANIEL AMVAME NZE

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: UnBLabRedes.MFE.037/2015

BRASÍLIA, DF: JULHO / 2015.

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ANÁLISE COMPARATIVA DE FERRAMENTAS DE GERENCIAMENTO DE CONTEÚDO VISANDO O COMPARTILHAMENTO SEGURO DE INFORMAÇÕES CORPORATIVAS

CARLO ALESSANDRO MELO NOCE

MONOGRAFIA DE ESPECIALIZAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO TÍTULO DE ESPECIALISTA EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

_____

GEORGES DANIEL AMVAME NZE
DR., UNB/ENE (ORIENTADOR)

_____

EDNA DIAS CANEDO
DRA., UNB/ENE (EXAMINADOR INTERNO)

_____

ELIANE CARNEIRO SOARES
MSC., SEDF (EXAMINADOR EXTERNO)

BRASÍLIA, DF, 14 DE JULHO DE 2015.

FICHA CATALOGRÁFICA

Noce, Carlo Alessandro Melo Noce.
Análise comparativa de ferramentas de gerenciamento de conteúdo visando o compartilhamento seguro de informações corporativas [Distrito Federal], 2015.
Xvi, 92p., 210 x 297mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2015).
Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.

1. BYOD	2. COBIT
3. ITIL	4. Segurança da Informação
5. Gerenciamento de Conteúdo	6. Mobilidade Corporativa
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

Noce, Carlo Alessandro Melo Noce. (2015). Análise comparativa de ferramentas de gerenciamento de conteúdo visando o compartilhamento seguro de informações corporativas. Monografia de Especialização, Publicação UnBLabRedes.MFE.037/2015, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 92p.

CESSÃO DE DIREITOS

AUTOR: Carlo Alessandro Melo Noce

TITULO DA MONOGRAFIA: Análise comparativa de ferramentas de gerenciamento de conteúdo visando o compartilhamento seguro de informações corporativas.

TÍTULO / ANO: Especialista / 2015

_____

Carlo Alessandro Melo Noce
SQNW 110 Bloco E Apt. 220 – Ed. Viverde, Noroeste.
CEP: 70.686-525 - Brasília - DF
Tel. 55 – 61 – 4141-9013 / alessandro_mn@hotmail.com

DEDICATÓRIA

Dedico esta monografia a Jesus Cristo, por estar sempre presente em minha vida e aos meus pais e familiares, pois deram todo o apoio e o suporte necessário para vencer mais uma batalha em minha vida.

Carlo Alessandro Melo Noce

AGRADECIMENTOS

A Deus, pois Ele guiou e continua a guiar o meu caminhar.

Ao meu orientador Prof. Doutor Georges Daniel Amvame-Nze, por estar sempre me incentivando e apoiando no desenvolvimento deste trabalho e na minha evolução como profissional.

Aos meus pais e família, pelo constante incentivo e dedicação que estão sempre me dando.

"O temor do Senhor é o princípio da sabedoria; bom entendimento têm todos os que cumprem os Seus mandamentos; o Seu louvor permanece para sempre." ***Salmo 111:10***.

RESUMO

ANÁLISE COMPARATIVA DE FERRAMENTAS DE GERENCIAMENTO DE CONTEÚDO VISANDO O COMPARTILHAMENTO SEGURO DE INFORMAÇÕES CORPORATIVAS

Autor: Carlo Alessandro Melo Noce
Orientador: Professor Georges Daniel Amvame-Nze
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 14 de JULHO de 2015.

Com o avanço da Tecnologia da Informação (TI), uma nova revolução chamada de mobilidade surge para dominar as informações das organizações e transformar o comportamento humano. Os *smartphones*, dispositivos móveis que gerenciam dados dos usuários e que estão trazendo praticidade para o negócio das empresas, impulsionaram a utilização dessa nova tendência. Com isso, a estratégia da mobilidade da informação contempla o fato de que os funcionários utilizem aparelhos móveis para realizar as suas tarefas gerando assim, serviços dinâmicos e produtividade. É nesse cenário que aparece no meio corporativo o termo BYOD (*Bring Your Own Device*). Logo, o estudo em questão tem como objetivo principal apresentar uma análise comparativa de ferramentas de gerenciamento de conteúdo que possam organizar, gerenciar, armazenar e controlar, conforme a demanda da corporação, o fluxo de dados empresarial. Verificar as ferramentas que melhor se adequem ao processo de segurança de serviços e de segurança da informação, de acordo com as normativas e melhores práticas do COBIT 5 e do ITIL v3, respectivamente. A fim de se ter o conhecimento para introduzir dentro da organização a plataforma ideal para o compartilhamento seguro das informações e assim, obter soluções de produtividade móvel com segurança e em nível corporativo.

ABSTRACT

COMPARATIVE ANALYSIS OF CONTENT MANAGEMENT TOOLS AIM AT SECURITY SHARING OF CORPORATE INFORMATION

With the advancement of Information Technology (IT), a new revolution call by mobility comes to dominate the information of organizations and transform human behavior. Smartphones, mobile devices that manage user data and are bringing convenience to the business of the companies, boosted the use of this new trend. Thus, information mobility strategy includes the fact that employees use mobile devices to make their tasks generating dynamic services and productivity. It is in this scenario that appears in the corporate environment the term BYOD (Bring Your Own Device). Therefore, the present study aims to present a comparative analysis of content management tools that can organize, manage, store and control, according to the corporate demand, the flow of business data. Check the tools that best suit to the security services and information security process in accordance with regulations and best practices of COBIT 5 and ITIL v3, respectively. In order to have the knowledge to introduce into the organization the ideal platform for the secure sharing of information and thus this get mobile productivity solutions safely and at the corporate level.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

AD/LDAP	*Active Directory/Lightweight Directory Access Protocol*
AES	*Advanced Encryption Standard*
AGPLv3	*Affero General Public License* - Versão 3
AJAX	*Asynchronous Javascript and XML*
ANO	Acordo de Nível Operacional
ANS	Acordo de Nível de Serviço
API	*Application Program Interface*
BBITG2e	*Board Briefing on IT Governance 2nd Edition*
BMIS	*Business Model for Information Security*
BYOD	*Bring Your Own Device*
CSS	*Cascading Style Sheets*
COBIT 5	*Control Objectives for Information and Related Technology* - Versão 5
DDS	*Deliver, Service and Support*
FIPS	*Federal Information Processing Standard*
GUI	*Graphical User Interface*
HTML	*HyperText Markup Language*
IN MP/SLTI N° 04	Instrução Normativa do Ministério do Planejamento, Orçamento e Gestão/Secretaria de Logística e Tecnologia da Informação número 04
IPS	*Intrusion Prevent System*
ISACA	*Information System Audit and Control*
ITAF	*Information Technology Assurance Framework*
ITIL v3	*Information Technology Infrastructure Library* - Versão 3
MDM	*Mobile Device Management*
NBR ISO/IEC	*International Organization for Standardization*
OGC	*United Kingdom's Office Of Government Commerce*
PDCA	*Plan - Do - Check – Act*
PHP	*Personal Home Page or Hypertext Preprocessor*
PMBOK	*Project Management Body of Knowledge*
PRINCE2	*PRojects IN Controlled Environments*
RACI	*Responsible, Accountable, Consulted and Informed*

Risk IT	*Risk of Information Technology*
SCL	*Secure Content Locker*
SGSI	Sistema de Gestão de Segurança da Informação
SLA	*Service Level Agreement*
SSL	*Secure Socket Layer*
TFG	*Taking Governance Forward*
TI	Tecnologia da Informação
TOGAF	*The Open Group Architecture Framework*
Val IT	*Value of Information Technology*
VPN	*Virtual Private Network*

1 – INTRODUÇÃO

A constante e crescente demanda por mobilidade trouxe para a área de TI diversos desafios, os quais passaram a relacionar-se com o mundo dos negócios. Ou seja, dispositivos móveis começam a ser inseridos no contexto das organizações, sendo esses equipamentos utilizados para todo tipo de demanda institucional. Logo, a mobilidade começa a fazer parte da estratégia de TI, envolvendo assim os sistemas corporativos e toda a informação que trafega na rede da empresa.

É nesse cenário que surge o termo *Bring Your Own Device* (BYOD). Colaboradores começam a utilizar dispositivos móveis pessoais para a realização das diversas atividades da corporação.

1.1 - CONTEXTUALIZAÇÃO

Cada empresa possui características específicas do seu negócio, sendo essencial dentro da área de TI uma Divisão de Segurança da Informação. Essa nova divisão possibilitará o fornecimento, dentro das suas políticas de segurança, de novas regras para utilização, monitoramento, integração e gerenciamento dos diversos dispositivos móveis que constantemente entram e saem da corporação.

Logo, para a estratégia de mobilidade, poderão ser combinados vários mecanismos de segurança para um gerenciamento eficaz do usuário que estiver realizando acessos e tarefas na rede corporativa. Como por exemplo: restrições de chamadas e de mensagens e acesso seguro ao compartilhamento de informações na *intranet* e *Internet* (serviços de nuvem, *e-mails*, aplicativos etc.).

Em suma, as corporações dependem de uma solução capaz de gerenciar de maneira segura e unificada as informações do negócio, fornecendo controle sobre os aplicativos e dispositivos móveis e proteção à rede corporativa. E, com a política de segurança bem elaborada, bem divulgada e de fácil entendimento, a Divisão de Segurança da Informação estará qualificada para combater as vulnerabilidades e as ameaças que geram diversos riscos ao negócio afetando toda a empresa.

1.2 - MOTIVAÇÃO

Elencar ferramentas de gerenciamento de conteúdo que tenham como base as Normas ISO/IEC 27001 e ISO/IEC 27002 e que estejam de acordo com a biblioteca de melhores práticas ITIL v3 e com o *framework* COBIT 5 com a finalidade de auxiliar as corporações no sucesso do negócio de TI. Outras motivações são listadas a seguir:

- Apresentar soluções que forneçam o compartilhamento seguro de informações para ambientes corporativos;
- Expor os melhores meios que facilitem, dentro do ambiente corporativo, o compartilhamento dos dados empresariais e que forneçam produtividade móvel com segurança ao negócio; e
- Propor soluções de segurança móvel para o ambiente corporativo, bem como, políticas de BYOD para utilização dos dispositivos móveis dentro da empresa.

A Figura 1.1 exemplifica a importância da aplicação de um programa de BYOD para prover segurança à rede de dados por meio de procedimentos básicos de utilização dos diversos dispositivos portáteis nas corporações.

Figura 1.1 - Modelo de segurança em redes BYOD. [Kaseya Blog (2013)]

1.3 - OBJETIVOS DO TRABALHO

A seguir serão descritos os objetivos gerais desta pesquisa, as metas de longo prazo, as contribuições deste trabalho e, como objetivos específicos, o detalhamento das tarefas propostas para este estudo.

1.3.1 - Objetivo Geral

O foco deste estudo consiste em apresentar uma análise comparativa das ferramentas de gerenciamento de conteúdo que possam organizar, gerenciar, armazenar e controlar todo fluxo de dados corporativo e, assim, permitir que os colaboradores tenham mobilidade com segurança ao manipular as informações da corporação.

1.3.2 - Objetivos Específicos

Para se alcançar o objetivo geral deste trabalho, será necessário detalhar assuntos pertinentes à pesquisa proposta, são eles:

- O entendimento da família de normas ISO 27000 mostrará como uma corporação poderá implementar um SGSI e uma política de segurança da informação;
- O estudo da biblioteca ITIL v3 trará a visão necessária para seguir as orientações propostas nela e aplicar as melhores práticas em todo o processo integrado de GSI da corporação;
- O estudo do *framework* CobiT 5 fornecerá uma série de recursos que servirão como um modelo de referência para gestão da área de TI empresa, assegurando a segurança dos diversos serviços do negócio; e
- Verificar as ferramentas que melhor se adequam ao processo – Gerenciamento de Serviços de Segurança – do *framework* CobiT 5 e ao processo – Gestão de Segurança da Informação (GSI) – da biblioteca de melhores práticas ITIL v3. E, com isso, ter como base as normas ISO 27001 e ISO 27002 que fornecerão os requisitos e as boas práticas necessárias para implementar a melhor solução de produtividade móvel com segurança para ambientes corporativos.

Por fim, a escolha das ferramentas delimitará melhor a pesquisa proposta e, após realizar o levantamento dos itens a serem avaliados, o quadro comparativo trará a visão do benefício de se implantar uma ferramenta de gerenciamento de conteúdo em uma organização, visto que a mobilidade do negócio necessita de um compartilhamento seguro das suas informações.

1.4 - METODOLOGIA DE PESQUISA

A metodologia de pesquisa proposta foi dividida em 3 fases para facilitar o entendimento do trabalho, conforme apresentado a seguir.

A divisão em fases tem por finalidade aprofundar e direcionar o estudo relacionado ao tema e ao problema proposto neste trabalho, orientado nos passos necessários para implementação de um SGSI, seguindo o fluxo do ciclo PDCA da Norma ISO/IEC 27001, e assim, fornecendo as regras e as estratégias para implantar uma política de BYOD na corporação.

Fase 1: Compreender o que é um SGSI, qual a sua finalidade dentro da corporação, como realizar a sua implementação e quais benefícios a corporação obterá com um sistema de gestão.

Fase 2: Entender como o ciclo PDCA influencia na implementação de um SGSI, como esse processo iterativo pode guiar as partes envolvidas nas tomadas de decisão e ter um fluxo de passos para constantemente melhorar e aperfeiçoar o SGSI.

Fase 3: Analisar dados estatísticos de empresas de mobilidade sobre BYOD nas corporações, compreender a importância de se implantar um programa de BYOD e listar as orientações necessárias para se obter sucesso na sua implantação dentro da corporação.

1.5 - CONTRIBUIÇÕES DO TRABALHO

Buscam-se com este trabalho as seguintes contribuições:

- Apresentação do atual cenário em que este trabalho é escrito e como a mobilidade corporativa pode trazer benefícios para todas as partes envolvidas com o negócio;
- Apresentação das principais bibliotecas e Normas de governança e gestão de TI, o que elas tratam sobre segurança da informação e como adequar a corporação com as suas recomendações;

- Apresentação de ferramentas de gerenciamento de conteúdo para ambientes corporativos, analisando suas características, funcionalidades e praticidades;
- Apresentação de uma proposta de uma Política de Segurança da Informação BYOD para o ambiente corporativo; e
- Verificar as ferramentas que melhor se adequam à área de Segurança da Informação das bibliotecas e Normas estudadas e quais dentre elas fornecem à corporação compartilhamento seguro de informações e produtividade móvel com segurança.

1.6 - ORGANIZAÇÃO DO TRABALHO

Para um melhor entendimento, este trabalho, será dividido em 4 (quatro) capítulos, descritos da seguinte forma:

No capítulo 2 será visto a fundamentação teórica, que fornecerá a base para a pesquisa proposta. Nos seus tópicos, serão apresentadas rápidas referências à família das normas ISO 27000, serão descritos sucintamente os aspectos relacionados à biblioteca ITIL v3, com foco no processo de GSI que está inserido no estágio Desenho de Serviço e será exposto um resumo do *framework* CobiT 5, dando ênfase no processo – Assegurar a Segurança dos Serviços – que faz parte do domínio Entregar e Suportar.

O capítulo 3 tratará da metodologia da presente proposta de pesquisa, ou seja, serão detalhadas as ferramentas de Gerenciamento de conteúdo e a segurança que elas proporcionam à corporação na utilização dos dispositivos móveis para troca de conteúdo.

No capítulo 4 serão apresentados os resultados da pesquisa realizada, bem como, a proposta da melhor ferramenta que atenda aos objetivos da corporação.

Após todas essas análises, o trabalho será concluído e propostas para futuros trabalhos serão apresentados no capítulo 5.

2 – ESTADO DA ARTE E REVISÃO BIBLIOGRÁFICA

Neste capítulo serão apresentados em seções as 3 (três) principais bibliotecas, no momento deste projeto, da área de TI e que possuem na sua estrutura os meios necessários para gerenciar com segurança as informações corporativas, trazendo assim, melhorias contínuas para o negócio.

Na seção 2.1 serão abordadas as Normas ISO/IEC 27000:2013, ISO/IEC 27001:2013 e ISO/IEC 27002:2013, pois definem de forma mais detalhada como introduzir na organização um SGSI.

Na seção 2.2 será descrito o guia de boas práticas ITIL v3, com foco no processo de GSI que faz parte do estágio Desenho de Serviço, segundo ITIL v3 (2011). E, por fim, na seção 2.3 um breve resumo do *framework* CobiT 5 será mencionado, sendo que sua ênfase estará no processo Gerenciamento de Serviços de Segurança que está inserido no domínio Entrega, Serviço e Suporte, segundo CobiT 5, ISACA (2012).

Após o entendimento dos conhecimentos listados acima, a etapa de escolha e definição das ferramentas de gerenciamento de conteúdo será mais eficaz, tendo em vista que os principais assuntos sobre Segurança da Informação foram estudados.

2.1 - FAMÍLIA ISO 27000

A família ISO 27000 constitui um padrão de certificação de sistemas de gestão desenvolvido pelo *International Organization for Standardization* (ISO), sua representação é feita por uma logo como mostra a Figura 2.1.

Figura 2.1 - Série ISO 27000:2013. [IT Governance Online (2015)]

Ela possui como introdução a ISO/IEC 27000:2013 que é uma visão geral das Técnicas e Gestão de Segurança e que auxilia no melhor estudo de cada uma das Normas dessa família. Pois apresenta na sua estrutura um glossário com definições e termos fundamentais utilizados no decorrer da série 27000.

Essa família de Normas fornece os conceitos que definem os requisitos para implantação de um SGSI e dão a base e a orientação de forma detalhada para os processos do ciclo *Plan-Do-Check-Act* (PDCA). Esse ciclo é o principal método iterativo de gestão e que possui 4 (quatro) etapas para um melhor controle e melhoria contínua de processos e produtos.

Essa série ISO serve de apoio e base às diversas organizações tanto do setor público quanto do setor privado. Ela norteia na compreensão dos princípios, fundamentos e demais conceitos proporcionando uma melhor gestão dos ativos (definição na subseção abaixo) que envolvem a informação.

A seguir serão listadas todas as Normas que são definidas pela série ISO 27000:

- Norma ISO 27000 – trata do vocabulário de Gestão de Segurança da Informação;
- Norma ISO 27001 – fornece um modelo capaz de estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI;
- Norma ISO 27002 – guia de boas práticas que descreve os objetivos de controle recomendados para a Segurança da Informação;
- Norma ISO 27003 – aborda diretrizes para a implementação de Sistemas de Gestão de Segurança da Informação e contém informações sobre como usar o modelo PDCA e os requisitos das suas diferentes fases;
- Norma ISO 27004 – especifica métricas e técnicas de medição aplicáveis para determinar a eficácia do SGSI;
- Norma ISO 27005 – estabelece diretrizes para a gestão de risco em Segurança da Informação, fornecendo indicações para implementação, monitorização e melhoria contínua do sistema de controles; e
- Norma ISO 27006 – especifica requisitos e fornece orientações para as instituições que realizam serviços de auditoria e certificação de um SGSI.

A Figura 2.2 apresenta um resumo de cada uma das Normas dessa série, sendo destacada a sua Norma base a ISO/IEC 27001:2013.

Figura 2.2 - Família ISO 27000 detalhada. [NEUPART (2015)]

2.1.1 - ISO/IEC 27000:2013

O principal objetivo da Gestão de Segurança da Informação é prover a qualidade das informações de uma determinada organização. Sendo que para se obter esse aspecto, três primícias fazem-se necessárias, a confidencialidade, a integridade e a disponibilidade. Essas características fazem parte e estão definidas na Norma ISO/IEC 27000:2013 que é um padrão global de definições para o gerenciamento de Segurança da Informação.

Para utilização de qualquer padrão, faz-se necessário ter como base um vocabulário que seja claramente definido para que sejam evitados problemas interpretações de gestão e de conceitos técnicos. Portanto, este estudo se baseia na Norma ISO/IEC 27000:2013 e a seguir serão apresentados alguns dos termos e definições aplicados por essa Norma e que auxiliarão no estudo proposto:

- Ação corretiva – ação para eliminar a causa de uma não conformidade detectada ou outra situação indesejável;
- Ameaça – causa potencial de um incidente indesejado, o que pode resultar em danos para um sistema ou entidade;
- Análise de risco – uso sistemático de informações para identificar fontes e estimar a ocorrência de um risco;
- Atacar – tentar destruir, alterar, expor, inutilizar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo;
- Ativos – qualquer coisa que tenha valor para a organização (informação, software, o próprio computador, serviços, as pessoas, entre outros);
- Autenticação – prestação de garantia de que uma característica reclamada por uma entidade é correta;
- Autenticidade – propriedade que nos diz que uma entidade é aquilo que realmente afirma ser;
- Controlar – meio de gestão de risco, incluindo as políticas de procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou de natureza legal;
- Controle de acesso – meios para assegurar que o acesso a ativos está autorizado e restringido com base no trabalho e em requisitos de segurança;
- Confidencialidade – propriedade que garante que a informação não está disponível ou revelada a indivíduos não autorizados, entidades ou processos;
- Diretriz – recomendação do que é esperado que seja feito a fim de alcançar um objetivo;
- Disponibilidade – propriedade de ser acessível e utilizável por uma entidade autorizada;
- Evento – ocorrência de um determinado conjunto de circunstâncias;
- Gestão de risco – atividades coordenadas para dirigir e controlar uma organização em relação a um determinado risco;

- Integridade – propriedade de proteger a exatidão de ativos;
- Política – regras, normas e requisitos formalmente expressos pela gestão e alinhados aos objetivos estratégicos;
- Processo – conjunto de atividades inter-relacionadas ou interativas que transformam insumos em produtos;
- Responsabilidade – responsabilidade de uma entidade pelas suas ações e decisões;
- Risco- combinação da probabilidade de um evento e das suas consequências;
- Risco de Segurança da Informação – potencial que uma ameaça explore uma vulnerabilidade de um ativo ou grupo de ativos e, assim, causar danos à organização;
- Segurança da Informação – preservação da confidencialidade, integridade e disponibilidade das informações;
- Sistema de Gestão – âmbito das políticas, procedimentos, diretrizes e recursos associados para alcançar os objetivos de uma organização;
- Sistema de Gestão de Segurança de Informação – parte do sistema de gestão global, com base numa abordagem de risco de negócio, para estabelecer, implementar, operar, monitorar, rever, manter e melhorar a segurança da informação; e
- Vulnerabilidade – fraqueza de um ativo ou controle, que pode ser explorado por uma ameaça.

A Norma ISO/IEC 27000:2013 possui os seguintes benefícios fundamentais:

- Aumento de segurança relativamente à gestão de processos;
- Confiança e regras claras para todos os envolvidos de uma organização;
- Conformidade com a legislação vigente sobre informação pessoal, propriedade, intelectual e outras;
- Estabelecimento de uma metodologia clara de Gestão da Segurança;
- Garantia de qualidade e confidencialidade comercial;

- O acesso à informação é feito por meio de medidas de segurança;
- Os riscos e os seus controles são continuamente verificados; e
- Reduzir o risco de perda, roubo ou alteração da informação.

2.1.2 - ISO/IEC 27001:2013

Segundo a ISO/IEC 27001:2013, esta Norma foi elaborada para especificar os requisitos que melhor definem um SGSI: estabelecimento, implementação, operacionalização, monitorização, revisão, manutenção preventiva e corretiva e melhoria contínua. Pontos esses que estão relacionados ao cenário dos riscos do negócio da empresa.

Algumas perguntas podem ser elencadas antes de se iniciar a implementação da norma em um sistema. São elas:

- Quais as áreas mais importantes dentro da organização que esta deve levar em consideração a fim de alcançar uma implementação de um SGSI de sucesso?
- Quais as consequências se a informação for utilizada indevidamente ou sem autorização?
- Quais os princípios básicos uma empresa deve-se nortear para realizar uma avaliação dos riscos?
- Qual o custo caso haja redução da produtividade por falhas, erros de sistema ou utilização de incorreta da informação?
- Qual o impacto da ocorrência de incidentes sobre as informações de uma organização? e
- Qual será o custo caso uma falha implique na perda efetiva de informação?

Após responder o questionário acima, uma organização terá uma maior aplicabilidade e uma probabilidade mais elevada de sucesso na implementação da Norma ISO/IEC 27001:2013. Inserir essa norma na empresa aumenta-se o foco nas necessidades do negócio e introduz, como parte integrante dos seus objetivos, a segurança da informação para gerir a gestão dos riscos.

Por ser universal, a ISO/IEC 27001:2013 contempla organizações públicas, privadas, governamentais, comerciais, com ou sem fins lucrativos etc. Essa Norma define

os requisitos básicos para a implementação de controles de segurança da informação personalizados às diversas necessidades de cada instituição.

A Norma ISO/IEC 27001:2013 engloba pontos relevantes e que são descritos a seguir para um melhor entendimento da sua estrutura:

1. Definição do Sistema de Gestão de Segurança da Informação:

- Estabelecer o SGSI;
- Implementar e Operar o SGSI;
- Monitorar e analisar criticamente o SGSI;
- Manter e melhorar o SGSI;
- Levantar requisitos para documentação; e
- Realizar controle contínuo de documentos e registros.

2. Responsabilidades da alta direção:

- Competência;
- Comprometimento;
- Conscientização do negócio;
- Gestora e fornecedora de recursos (financeiros); e
- Treinamento e capacitação constante.

3. Auditorias internas que validam a correta implantação de um SGSI:

- Atender aos requisitos da norma;
- Estar de acordo com os requisitos de segurança elencados; e
- Perfeito funcionamento conforme estabelecido na norma.

Todo e qualquer procedimento realizado em uma auditoria deve ser previamente documentado para futuras análises e os auditores não podem auditar o seu próprio negócio, garantindo assim, imparcialidade e objetividade.

4. Análise crítica do SGSI pela alta direção:

- Ponto de entrada: resultado das auditorias e análises críticas, situação das ações preventivas e corretivas, vulnerabilidades não contempladas adequadamente nas análises anteriores, resultados, recomendações e mudanças; e
- Ponto de saída: oportunidade de incluir melhorias e mudanças, modificação do SGSI e das necessidades de recursos.

5. Melhoria contínua do SGSI:

- Melhoria contínua por meio do uso da política definida;
- Análise dos resultados colhidos pelas auditorias e pelos eventos monitorados; e
- Exclusão das não conformidades encontradas por meio de ações corretivas e preventivas.

A Norma ISO/IEC 27001:2013 possui um anexo A que é um normativo que faz referência aos seus controles e objetivos de controles. Esse anexo possui uma tabela que uma das suas seções trata da Organização da Segurança da Informação e tem um tópico voltado para dispositivos móveis e trabalhos remotos. O objetivo desse tópico segundo a Norma ISO/IEC 27001:2013 é garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis e seus dois itens são descritos da seguinte forma:

- Política para o uso de dispositivo móvel – Controle: uma política e medidas que apoiam a segurança da informação devem ser adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis; e
- Trabalho remoto – Controle: uma política e medidas que apoiam a segurança da informação devem ser implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.

Com o estudo realizado das Normas ISO/IEC 27000:2013 e ISO/IEC 27001:2013 pode-se concluir que a primeira aparece como uma maneira de se definir termos e conceitos para uma futura implementação de um SGSI. Enquanto que a segunda, apresenta requisitos básicos, porém fundamentais, que fornecem alguns procedimentos para uma Gestão de Segurança da Informação eficaz. Logo, um plano de controle previamente definido facilitará todos os passos para implementação desse sistema de gestão.

2.1.3 - ISO/IEC 27002:2013

A Norma ISO/IEC 27002:2013 é a atualização da norma ISO/IEC 17799:2005, e descreve na sua estrutura os procedimentos para implementar um código de boas práticas para a Gestão da Segurança da Informação, definindo técnicas de segurança para a TI.

Segundo a ISO/IEC 27002:2013, esta Norma estabelece diretrizes e princípios gerais para estabelecer, implementar, monitorar, analisar criticamente, manter e melhorar um SGSI em uma organização. Os objetivos definidos nesta Norma proveem diretrizes gerais sobre as metas geralmente aceitas para a Gestão da Segurança da Informação.

A principal característica desta Norma é ser um guia de fácil entendimento e usabilidade para a elaboração de regras e métodos de segurança da informação para uma empresa. Dessa forma, a gestão da segurança fica cada vez mais eficiente e a visibilidade da organização no mercado passa a ser mais confiável.

Seus objetivos de controle têm como principal característica serem implementados para satisfazer os diversos requisitos que são coletados por meio da eficaz análise e varredura de riscos, os quais são encontrados na empresa e afetam o negócio.

Para os efeitos da Norma ISO/IEC 27002:2013, aplicam-se os termos e definições da Norma ISO/IEC 27000:2013.

Segundo a Norma ISO/IEC 27002:2013, sua estrutura contempla 14 seções de controles de segurança da informação, sendo que para este estudo, será analisado a seção Política de Segurança da Informação.

A Política de Segurança da Informação apoia e guia a alta direção da organização para se atentar à segurança da informação conforme os decretos e as leis públicas e institucionais e os objetivos do negócio. Logo, é necessário que a liderança da empresa defina uma política de fácil entendimento, que esteja de acordo com os requisitos do negócio e que a publique e revise-a constantemente a toda organização.

O documento da política ao ser aprovado pela alta direção, deve ser publicado e divulgado aos funcionários e terceiros, sendo de fácil acesso e entendimento. Sua estrutura deve conter o foco da empresa para gerenciar a segurança da informação, bem como:

- Declaração de comprometimento da liderança;

- Definição, escopo, metas globais, responsabilidades gerais e importância da segurança da informação;
- Descrição das punições no não cumprimento da política e de referências à documentação;
- Detalhamento de todos os princípios, requisitos e normas de segurança da informação (conscientização, treinamento e uso) alinhados à leis e regulamentos contratuais; e
- Objetivos de controles e gestão de riscos bem descritos.

A Norma ISO/IEC 27002:2013 por ser um código de boas práticas, descreve mais detalhadamente a Norma anterior a essa, a 27001:2013, e em um dos seus tópicos voltados a usuários finais, o tópico sobre dispositivos móveis e trabalho remoto visto na subseção anterior é também melhor desenvolvido nesta Norma para uma maior compreensão.

Segundo a Norma ISO/IEC 27002:2013, as principais diretrizes de implementação das políticas para uso de dispositivo móvel e para trabalho remoto são descritas a seguir:

1. Diretrizes de implementação para uso de dispositivo móvel: Convém que quando se utilizam dispositivos móveis, cuidados especiais sejam tomados para assegurar que as informações do negócio não sejam comprometidas. Convém que a política de dispositivos móveis leve em consideração os riscos de se trabalhar com esses dispositivos móveis em ambientes desprotegidos.

   Convém que a política para uso de dispositivos móveis considere:

   a) Registros dos dispositivos móveis;
   b) Requisitos para a proteção física;
   c) Restrições quanto à instalação de *softwares*;
   d) Requisitos para as versões dos *softwares* e aplicações de *patches*;
   e) Restrições para conexão aos serviços de informação;
   f) Controle de acesso;
   g) Técnicas criptográficas;
   h) Proteção contra códigos maliciosos;
   i) Desativação, bloqueio e exclusão de forma remota;

j) *Backups*; e

k) Uso dos serviços *web* e aplicações *web*.

2. Diretrizes para implementação de trabalho remoto: Convém que a organização que permita a atividade de trabalho remoto publique uma política que defina as condições e restrições para o uso do trabalho remoto. Quando considerados aplicáveis e permitidos por lei, convém que os seguintes pontos sejam considerados:

   a) A segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local;

   b) O ambiente físico proposto para o trabalho remoto;

   c) Os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acessada e trafegada na linha de comunicação e a sensibilidade do sistema interno;

   d) A provisão de acesso virtual às estações de trabalho dos usuários, para prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular;

   e) A ameaça de acesso não autorizado à informação ou aos recursos de processamento da informação por outras pessoas que utilizam o local, por exemplo familiares e amigos;

   f) O uso de redes domésticas e requisitos ou restrições na configuração de serviços de rede sem fio;

   g) Políticas e procedimentos para evitar disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular;

   h) Acesso a equipamentos de propriedade particular (para verificar a segurança da máquina ou durante uma investigação), que pode ser proibido legalmente;

   i) Acordos de licenciamento de *software* que podem tornar as organizações responsáveis pelo licenciamento do *software* cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou terceiros; e

   j) Requisitos de proteção contra vírus e requisitos de *firewall*.

Por fim, convém que a Política de Segurança da Informação seja periodicamente revisada por meio de uma análise crítica de forma a assegurar sua eficácia e contínua pertinência. Essa revisão será feita por um gestor escolhido pela alta direção e deve visar a melhoria da política e do negócio.

Na próxima seção será estudado como a biblioteca de boas práticas ITIL v3 propõe o uso do Gerenciamento de Segurança da Informação dentro da organização.

2.2 - ITIL V3

A biblioteca ITIL v3 é uma fonte de boas práticas usada para estabelecer e melhorar as capacidades no Gerenciamento de Serviço. É um guia aplicável a todos os tipos de organizações que provêm serviços ao negócio, sendo baseada no Ciclo de vida de Serviço. Em sua estrutura possui estágios complementares específicos para cada setor do mercado, considerando o que há de particular nos diversos segmentos das organizações (arquiteturas tecnológicas, modelos operacionais etc.).

Segundo MANSUR (2009: pg. 29), ITIL é um conjunto de orientações descrevendo as melhores práticas para um processo integrado do gerenciamento de serviços de TI que foi desenvolvido pela OGC, *United Kingdom's Office Of Government Commerce*, no final dos anos 80 para melhorar o gerenciamento dos serviços de TI do governo da Inglaterra.

Nas instituições, ITIL busca o alinhamento da TI aos requisitos do negócio por meio da entrega dos serviços e do suporte. Seu modelo tem referência mundial no gerenciamento dos serviços na área de TI, sendo o provimento desses serviços de TI por meio dos diversos ativos de informação da empresa (pessoas, infraestrutura de hardware, documentações, software etc.).

O modelo ITIL v3 é uma atualização da segunda versão que foi publicada na década de 90 sendo a versão atual lançada em 2011. O seu foco, como já foi descrito, está no gerenciamento de serviços de TI, e é com base nisso que o seu objetivo principal está em prover com melhor qualidade um serviço de TI que atenda às necessidades do negócio e, visando, em longo prazo, a mitigação de custos.

A Figura 2.3 exibe todo o ciclo de vida de um serviço de TI adotado pela ITIL v3, representando assim o Núcleo do ITIL e seus guias complementares.

Figura 2.3 - Ciclo de vida adotado pela ITIL v3. [ManagIT (2007)]

A seguir são listados os cinco livros que compõem essa nova versão do ITIL:

1. Estratégia de Serviços (*Service Strategy*);
2. Desenho de Serviços (*Service Design*);
3. Transição de Serviços (*Service Transition*);
4. Operação de Serviços (*Service Operation*); e
5. Melhoria Contínua de Serviços (*Continual Service Improvement*).

Com o objetivo de prover o direcionamento em como projetar e desenvolver serviços e processos para o Gerenciamento do Serviço, o estágio Desenho de Serviço é a principal etapa do ciclo de gerenciamento de serviços proposto pela ITIL. Seus princípios e métodos são capazes de transformar os objetivos estratégicos em portfólio de serviços e ativos estratégicos.

Sendo assim, o Desenho de Serviço trata no seu planejamento dos processos que estão diretamente relacionados às mudanças e às melhorias necessárias para aumentar ou manter o valor que os clientes obtêm dos serviços ao longo do ciclo de vida, garantindo os *Service Level Agreement* (SLAs) acordados no contrato. A seguir, esse processo é

detalhado para o entendimento dos seus conceitos e de que forma se relaciona com a área de gestão de TI.

2.2.1 - Desenho de Serviço

O estágio Desenho de Serviço do modelo ITIL v3 é a segunda fase do ciclo de vida, após a etapa Estratégia de Serviço. Por dar sequência ao andamento do fluxo proposto no nível estratégico, esse estágio proporciona um guia que relaciona as necessidades do negócio com a área de TI.

O seu foco está em orientar e auxiliar os diversos profissionais no uso de práticas e processos recomendados de Gerenciamento de Serviços de TI para criação e manutenção de políticas de TI, para o desenvolvimento de arquiteturas e de documentos que auxiliam no desenho dos serviços e de soluções inovadores de infraestrutura para os processos de TI.

Abaixo são listados os principais objetivos do Desenho de Serviço para o bom andamento do ciclo de vida:

- Contribuir para a melhoria continuada do serviço assegurando que uma qualidade do serviço está sendo implantada no ambiente de produção;
- Desenhar processos eficientes e eficazes para gerenciar o serviço durante seu ciclo de vida;
- Desenhar serviços que estejam alinhados e satisfaçam os objetivos do negócio;
- Desenhar serviços que são desenvolvidos dentro de uma escala de tempo e custo. Os serviços precisam ser entregues no prazo acordado e dentro do custo esperado;
- Desenhar uma infraestrutura segura e resiliente, ou seja, tolerante a falhas;
- Documentar planos, políticas, arquitetura e treinamento da equipe;
- Facilitar a introdução de serviços nos diversos ambientes da organização, garantindo a entrega da qualidade e a satisfação do cliente, preparando assim, para o próximo estágio (Transição de Serviços); e
- Gerenciar e identificar riscos, desenvolvendo um mapeamento completo de todo ciclo de vida.

Para um maior entendimento do processo de Desenho de Serviço, são listadas abaixo as suas atividades:

- Confecção e manutenção constante das políticas de TI e das documentações de desenho do serviço;
- Engenharia, levantamento de requisitos e análise para garantir que as exigências do negócio estejam devidamente documentadas e acordadas;
- Garantia de que todas as políticas e as estratégias do negócio e da TI estão alinhadas;
- Gerenciamento e avaliação de risco de todos os resultados e os processos do desenho de serviço;
- Informações, desenho de serviços e processos, métricas e tecnologias adequados para servir aos requisitos do negócio;
- Integração com todas as etapas, as atividades e os papéis de desenho do serviço;
- Revisão de todos os documentos de planejamento e desenho do serviço para a implantação de estratégias de TI usando mapeamento, projetos especiais e programas; e
- Revisão e análise de todos os processos e documentos envolvidos no estágio, incluindo políticas, planejamentos, desenhos e arquiteturas.

Para uma boa implantação do Gerenciamento de Serviços de TI, é necessário integrá-la com o planejamento e a preparação do uso eficiente e eficaz dos 4 Ps do modelo ITIL v3 que está focado nos fatores críticos de sucesso da organização.

Estes elementos demonstram competências primordiais que o provedor de serviços deve possuir para o bom funcionamento do ciclo de vida do serviço e do negócio.

Sem a integração dos 4 Ps, todo e qualquer projeto, desenho ou plano é prejudicado, pois haverá falta de gerenciamento e preparação.

A seguir são descritos os 4 Ps do Desenho de Serviço e na Figura 2.4 são listados seus respectivos exemplos:

- Pessoas – os papéis dos envolvidos nos processos deve ser bem definido;
- Processos – cada uma das etapas a serem desenvolvidas precisam ser bem planejadas e detalhadas;
- Produtos – são necessárias ferramentas para automatizar todos os processos e os serviços; e

- Parceiros – devem ser estabelecidos, pois são de extrema importância para compor a cadeia de serviços.

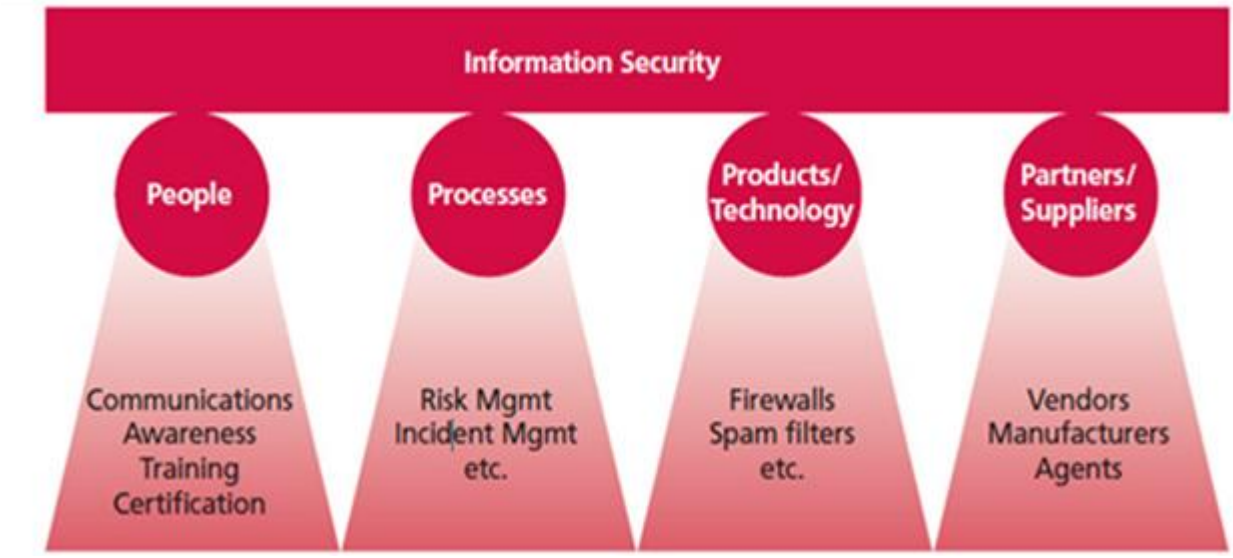

Figura 2.4 - Os 4 P's do Gerenciamento de Serviço do ITIL. [Webinsider (2014)]

O estágio Desenho de Serviço possui na sua estrutura 7 processos que atendem as diversas áreas da organização. A seguir são listados os processos:

- Gerenciamento de Nível de Serviço;
- Gerenciamento do Catálogo de Serviço;
- Gerenciamento da Disponibilidade;
- Gerenciamento da Segurança da Informação;
- Gerenciamento de Fornecedor;
- Gerenciamento da Capacidade; e
- Gerenciamento da Continuidade do Serviço de TI.

A Figura 2.5 apresenta o modelo de Gerenciamento do Serviço da biblioteca ITIL v3, demonstrando, dentro da corporação, como o serviço é tratado pela área de TI para prover o suporte aos seus usuários e a entrega para os seus clientes.

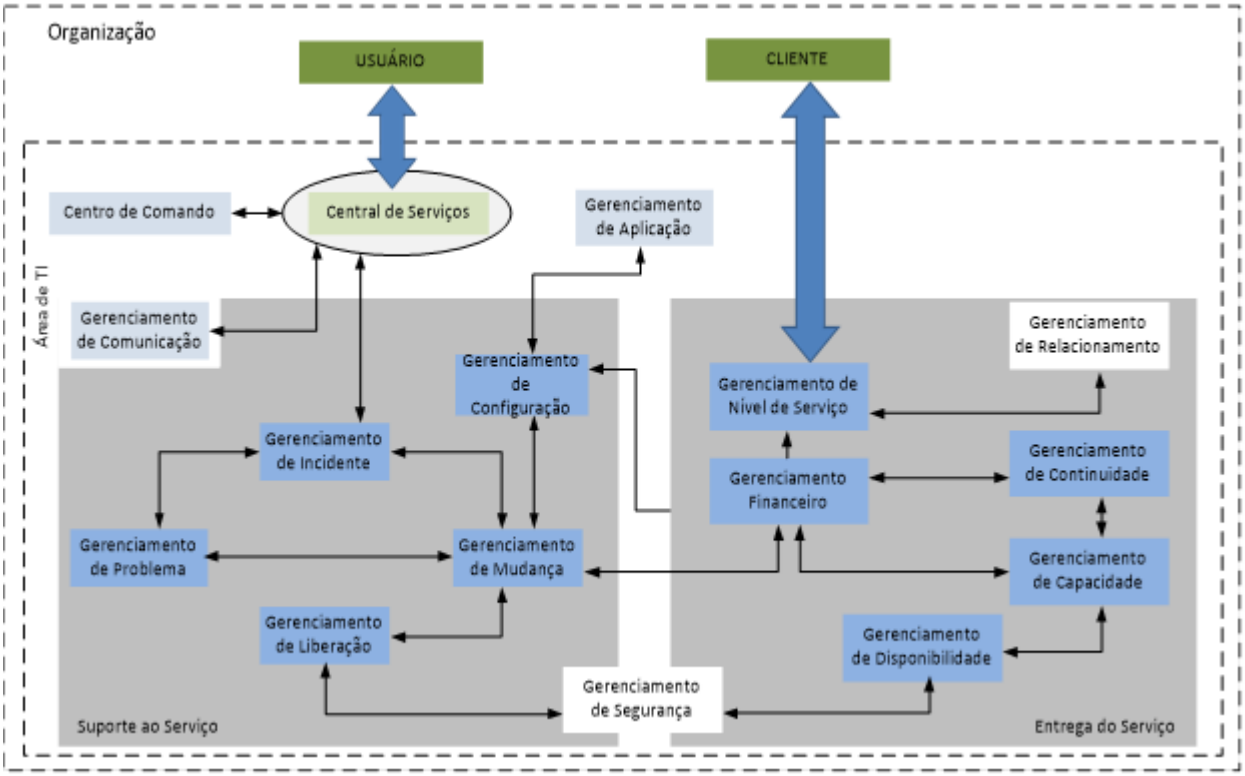

Figura 2.5 - Modelo de Gerenciamento do Serviço ITIL v3. [Magalhães (2007: pg. 108)]

Para um melhor entendimento do estudo proposto, o processo Gerenciamento da Segurança da Informação será descrito na subseção abaixo, visto que trata do controle e proteção das informações que impactam e fazem parte do negócio.

2.2.2 - Gerenciamento da Segurança da Informação

O Gerenciamento da Segurança da Informação é um processo do estágio Desenho de Serviço que visa controlar todo fluxo de informações, protegendo-os para não serem utilizados de forma indevida e não gerarem riscos para o negócio.

Atualmente a informação é um dos fatores críticos do negócio, sendo um dos ativos mais valiosos para a empresa. Com isso, a área de segurança da informação tem papel de extrema importância e relevância para a organização, lidando diretamente com a alta direção e toda a estratégia do negócio.

Como hoje em dia todos os dados estão sendo armazenados em soluções e aplicações de TI, há uma preocupação constante com ataques de *hackers*, entradas de *malwares*, e acessos não autorizados aos dados nos sistemas.

É com base nesse cenário que os objetivos do Gerenciamento da Segurança da Informação aparecem para auxiliar o gestor de TI da organização. A seguir são listados os objetivos desse processo:

- Confidencialidade dos dados – assegura que o acesso às informações seja feito de maneira correta, sendo acessadas somente por quem tem autorização;
- Integridade dos dados – garante que a informação, ao ser entregue, chegue no destino de forma precisa, protegida contra modificações e esteja completa;
- Disponibilidade dos dados – propriedade que valida que a informação estará sempre disponível para uso legítimo, ou seja, somente pelos usuários autorizados; e
- Autenticidade – confiabilidade das transações na troca de informações, garantindo e testificando sempre a fonte e a origem do dado, não sofrendo modificações ao longo do envio.

Devido as diversas e constantes pressões do mercado externo, é necessário que o Gerenciamento da Segurança da Informação defina controles de segurança aos dados atendendo assim os objetivos acima mencionados. Todavia, é fundamental prover um nível básico de segurança independente de requisitos externos, para que a operação da organização de TI e do negócio estejam sempre em perfeito funcionamento.

Como resultado desse processo, surgirá a Política de Segurança da Informação. Um documento que contém uma série de controles de segurança alinhados aos objetivos estratégicos da empresa e diversas conformidades para atender regulamentos e leis públicas e privadas. A política deve ser de fácil acesso por todos da instituição, portanto, ela deve ser difundida livremente em toda a empresa.

Essa política será validada pelo Gerente de Segurança, pessoa responsável por atestar que todos os objetivos do processo serão contemplados. Abaixo são listadas as suas principais responsabilidades:

- Confeccionar, atualizar e revisar constantemente a Política de Segurança da Informação;
- Anunciar e difundir a Política de Segurança da Informação para todas as partes envolvidas ao negócio, facilitando o acesso à documentação; e

- Assegurar que a política está realmente alinhada às estratégias do negócio, bem como, todos na instituição está obedecendo e seguindo seus requisitos.

De forma a facilitar a implantação da segurança da informação na empresa, a ITIL v3 baseou o processo de Gerenciamento da Segurança da Informação na Norma ISO/IEC 27001. Logo, essa ISO estabelece uma estrutura de etapas, conforme exibe a Figura 2.6, que devem ser seguidas para garantir a gerência da segurança de TI.

Figura 2.6 - Estrutura para gerenciar a segurança de TI. [Webinsider (2014)]

A seguir será detalhada cada uma das etapas, para melhor compreensão, da estrutura de Gerenciamento de Segurança de Tecnologia da Informação:

- Controlar – etapa inicial da atividade de Gerenciamento de Segurança, refere-se à administração e à organização do processo. Sua estrutura (*framework*) define funções de segurança, subprocessos e responsabilidades e papéis dos envolvidos. Ela descreve também os planos de ação da segurança (avaliações, planejamentos, acordos e a base organizacional);
- Planejar – etapa de planejamento da segurança em que são definidos o Acordo de Nível de Serviço (ANS) juntamente ao Gerenciamento de Nível de Serviço e os

contratos com terceiros. Os objetivos do ANS são especificados em um Acordo de Nível Operacional (ANO), ou seja, são definidos nos planos de segurança, sendo seus processos devidamente implantados e coordenados na organização;

- Implantar – passo em que são implantadas de forma objetiva todas as medidas (segurança de pessoal, classificação e gerenciamento de recursos de TI e gerenciamento da segurança) especificadas nos planejamentos;
- Avaliar – etapa na qual o desempenho dos processos é avaliado, de maneira a atualizar e validar as medidas acordadas e os níveis de segurança implantados. As avaliações são realizadas da seguinte forma: autoavaliação, auditorias internas e auditorias externas; e
- Manuter – etapa em que são feitas manutenções preventivas e corretivas, com base nos resultados da atividade de avaliação e de riscos, nos planos de segurança ANO e nas sessões de segurança definidas no ANS. Essas manutenções são necessárias devido as constantes mudanças que acontecem na infraestrutura de TI, nos processos do negócio e da organização etc.

Em suma, o Gerenciamento da Segurança da Informação é um grande aliado do Gerente de Segurança, pois sua estrutura fornece todos os meios e os requisitos necessários para atender as peculiaridades e as exigências que a segurança precisa e que já estão estabelecidas nos planos e políticas da organização.

Tudo isso é de extrema importância, pois evita que ocorram infrações nos controles de segurança, previne o negócio dos diversos riscos existentes e fortalece os alicerces, o avanço e a estrutura organizacional da empresa.

2.3 - COBIT 5

Estrutura de gestão e governança corporativa de TI, o CobiT 5 (*Control Objectives for Information and Related Technology*) é produzido e distribuído pela associação profissional e internacional ISACA (*Information System Audit and Control*), sendo sua última versão lançada no final de 2012.

Os diversos *frameworks* mundiais voltados para área de governança de TI, publicados pelo ISACA, estão integrados com o conteúdo (objetivos, domínios e processos) do CobiT 5. São eles: Val IT, Risk IT, BMIS, ITAF, TFG e BBITG2e. Além

disso, sua estrutura está alinhada aos demais padrões de TI do mercado mundial como, por exemplo: ITIL v3, ISO, PMBOK, PRINCE2 e TOGAF.

O CobiT 5 é considerado um parceiro para as empresas, pois ele gera valor para a TI, provendo o equilíbrio necessário entre a otimização dos níveis de uso de recursos e de riscos e a realização de benefícios para o negócio. A Figura 2.7 apresenta os principais objetivos desse *framework* e a seguir são descritas suas características:

- Conceder à TI o gerenciamento e a governança de sua totalidade em toda a organização;
- Desenvolver um protocolo comum de comunicação entre o negócio e a TI de acordo com a gestão e a governança corporativa; e
- Fornecer uma ampla estrutura de forma a auxiliar as organizações na potencialização do valor alcançado pela TI.

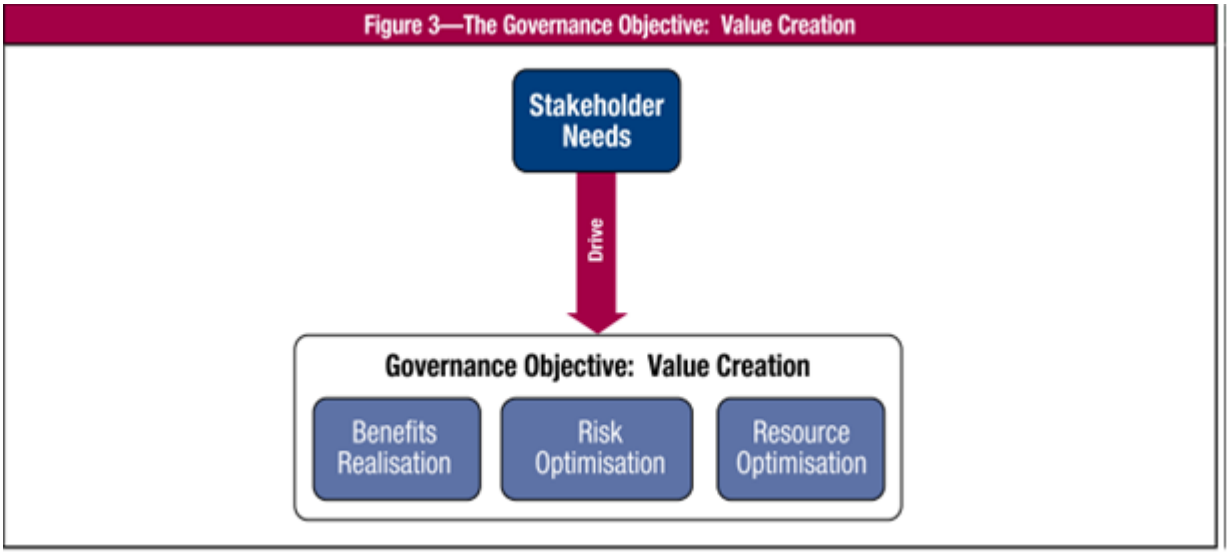

Figura 2.7 - Objetivo da Governança CobiT 5. [ISACA (2012)]

Em toda a organização a TI deve ser tratada como parte significante do negócio e a alta direção deve alinhar os planos estratégicos junto à área de tecnologia. Assim, haverá na empresa uma gestão e uma governança eficaz de todos os ativos de informação e do negócio, gerando valor, ou seja, resultados satisfatórios para todos os envolvidos. Logo, as necessidades dos *stakeholders* são transformadas em estratégias corporativas.

A Figura 2.8 exibe os 5 (cinco) princípios do CobiT 5 e a seguir são listados os principais benefícios que esse *framework* oferece para as empresas:

- Alcançar metas estratégicas e gerar valor dos investimentos feitos em TI;

- Customizar os gastos gerados pelos serviços de TI;
- Mitigar e combater constantemente os riscos que afetam aos ativos de informação e ao negócio;
- Obter alta qualidade operacional no uso eficiente e correto da tecnologia;
- Preservar as informações em alto nível a fim de resistir as tomadas de decisões do negócio; e
- Respeitar e seguir a conformidade com as leis, as políticas, os acordos contratuais, e os regulamentos.

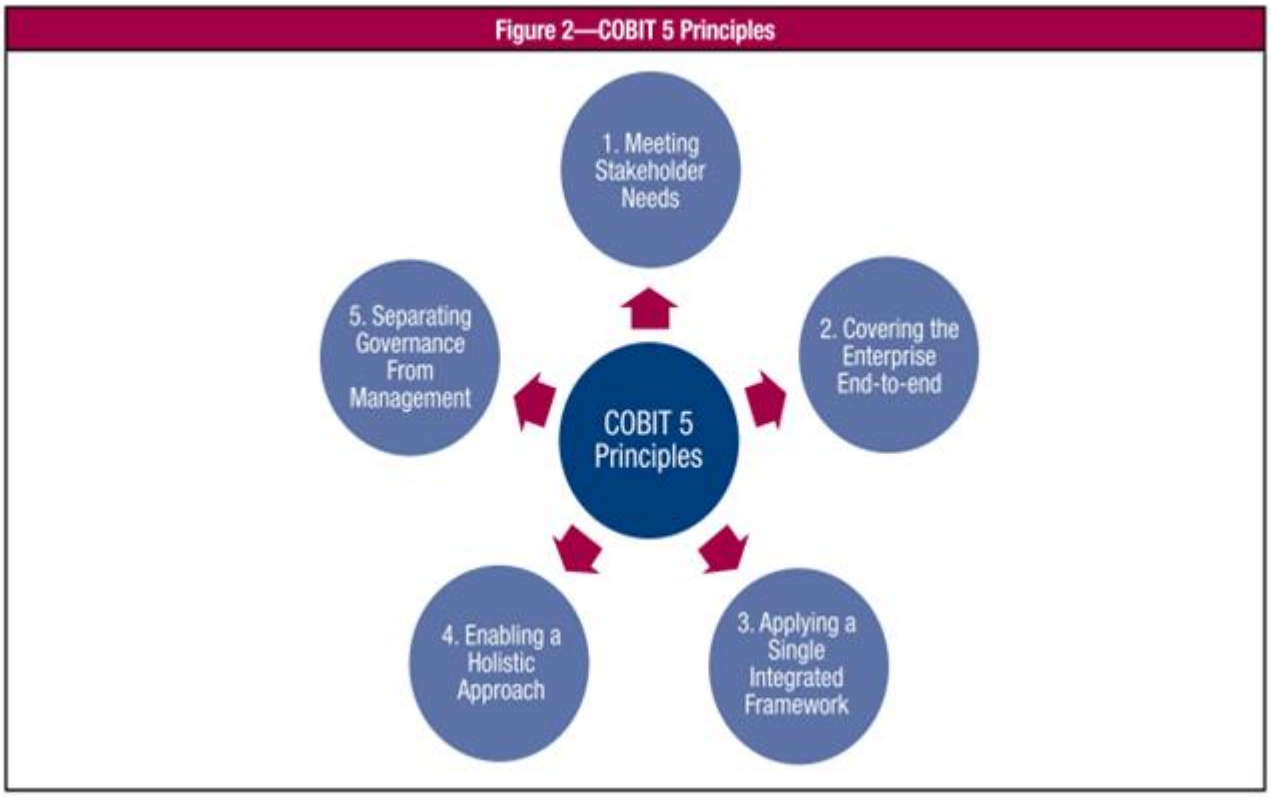

Figura 2.8 - Princípios do CobiT 5. [ISACA (2012)]

Segundo CobiT 5, ISACA (2012), a estrutura do modelo de governança tem como base 5 (cinco) princípios:

1. Atender as necessidades dos *stakeholders*;
2. Cobrir a organização de ponta a ponta;
3. Aplicar um framework único e integrado;
4. Possibilitar uma abordagem holística; e
5. Separar a governança da gestão.

O Modelo de Referência de Processos do CobiT 5 subdivide os 37 processos de TI em duas principais áreas de atividade – governança e gestão – que são divididas em domínios de processos.

Os 5 (cinco) processos de governança compõem o domínio - Avaliar, Dirigir e Monitorar (EDM) e os 32 processos de gestão compõem os 4 domínios:

- Alinhar, Planejar e Organizar (APO);
- Construir, Adquirir e Implementar (BAI);
- Entrega, Serviço e Suporte (DSS) e
- Monitorar, Avaliar e Medir (MEA).

O CobiT 5 fornece também uma matriz RACI (*Responsible, Accountable, Consulted and Informed*) para cada um dos seus processos descrevendo de forma detalhada e clara papéis e responsabilidades para prática de gestão, permitindo uma melhor definição das funções, das tarefas e dos níveis de envolvimento na concepção e implementação de processos.

Em síntese, essa nova versão do framework da ISACA tem o foco em governança corporativa de TI, ressalta cada vez mais o papel da alta administração nas tomadas de decisões tanto do negócio como da TI e auxilia no desenvolvimento de uma efetiva gestão e governança de TI que gera valor e benefícios, baseados nos planos estratégicos, aos *stakeholders*.

Portanto, o CobiT 5 provê um cenário ideal de apoio às organizações para atingirem suas metas e entregar valor por meio de uma efetiva governança e gestão da TI corporativa.

Para dar sequência à linha de raciocínio que está sendo proposta, será detalhado, na próxima subseção, o domínio Entrega, Serviço e Suporte (DSS).

2.3.1 - Entrega, Serviço e Suporte

O domínio Entrega, Serviço e Suporte - *Deliver, Service and Support* (DSS) -, faz parte do processo de Gestão do CobiT 5, e está de acordo com a área de executar a entrega dos serviços, fornecendo total apoio à TI. Essa entrega abrange as operações padrões sobre os aspectos de segurança, continuidade e treinamento.

Seu foco está em verificar constantemente se os serviços de TI estão alinhados às prioridades do negócio, se os custos estão otimizados, se existe confidencialidade, integridade e disponibilidade adequada e se as demandas de uso das aplicações de TI estão aceitáveis e seguras. A Figura 2.9 mostra o modelo de referência de processos para governança de TI utilizado pelo CobiT 5.

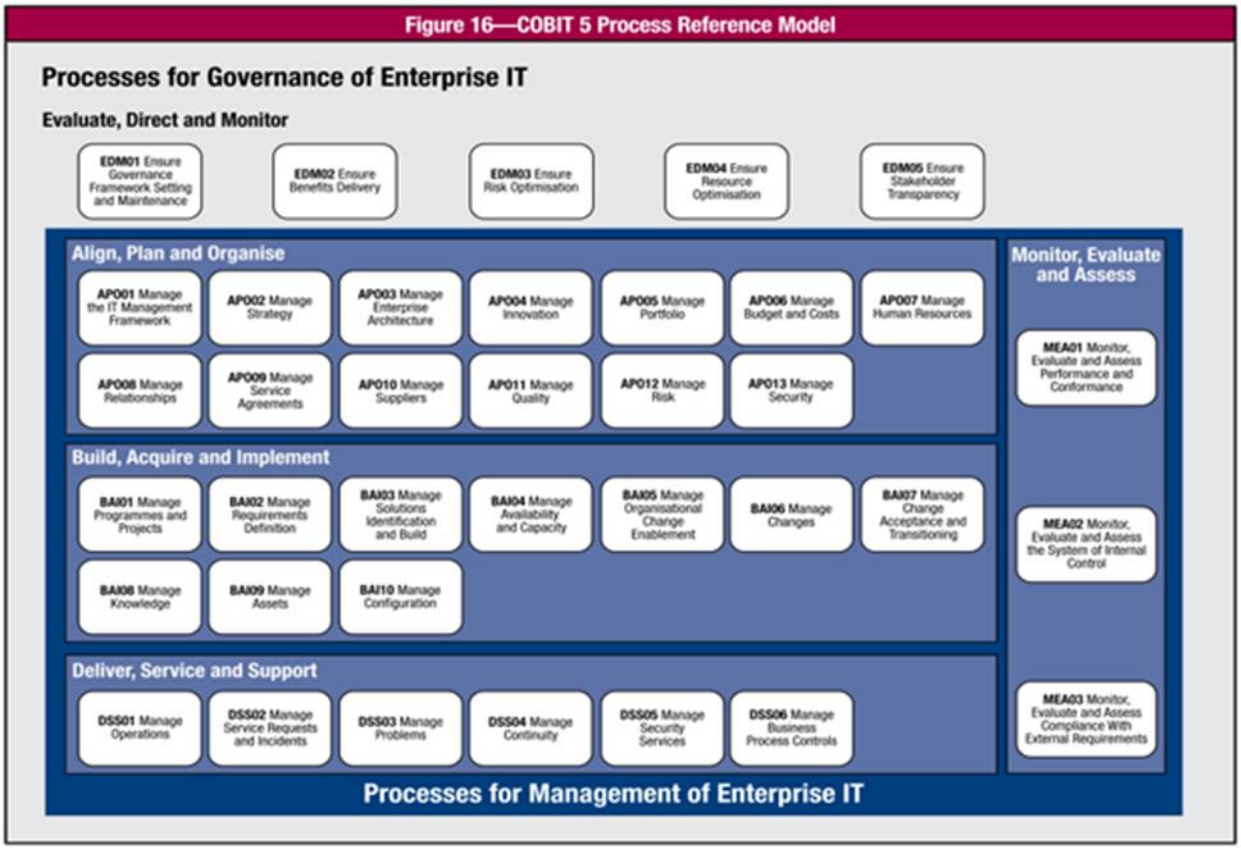

Figura 2.9 - Modelo de Referência de Processos CobiT 5. [ISACA (2012)]

O DDS visa atender a todos os planos estratégicos e táticos do negócio realizando à entrega dos serviços de TI acordados. Sua estrutura contempla 6 (seis) processos que impactam diretamente todo fluxo estratégico. São eles:

- Gerenciamento de operações - DDS01;
- Gerenciamento de requisições de serviços e incidentes - DDS02;
- Gerenciamento de problemas - DDS03;
- Gerenciamento de continuidade - DDS04;
- Gerenciamento de serviços de segurança - DDS05; e
- Gerenciamento de controle de processos do negócio - DDS06.

Logo, é nesse domínio que haverá o controle e as garantias de que os serviços estão sendo executados conforme o planejado e desenvolvido nos domínios anteriores do CobiT 5 e alinhados ao negócio.

Na próxima subseção será estudado o processo Gerenciar Serviços de Segurança, etapa na qual a gestão da segurança atua fortemente realizando controles para manter a integridade da informação, proteger os ativos de TI e minimizar o impacto de possíveis ataques e vulnerabilidades sobre o negócio.

2.3.2 - Gerenciamento de Serviços de Segurança

O processo Gerenciamento de Serviços de Segurança do domínio DSS visa proteger as informações da organização de forma a manter o nível de risco aceitável para a área de segurança da informação da empresa, tendo como base a política de segurança.

Suas principais características (objetivos) visam estabelecer e manter um alto padrão de segurança dos dados, definindo métodos e funções de segurança, privilégios de acesso e realizando monitoramentos físicos (de pessoas, ambientes e equipamentos) e lógicos (tráfego de dados da rede corporativa).

Para realizar a implementação desse processo é necessário definir alguns aspectos importantes para o negócio, quem são os *stakeholders*, quais são as suas responsabilidades e papéis no fluxo estratégico e quais políticas, regulamentos, padrões e procedimentos serão seguidos para aplicar de fato a segurança na organização.
O alcance dos objetivos será obtido com a execução de alguns passos:

- Compreender todos os ataques, as ameaças e as vulnerabilidades internas e externas que geram riscos ao negócio;
- Garantir que os dados físicos e lógicos estão sendo devidamente armazenados em ambientes seguros, e se ao serem transmitidos ou destruídos são feitos de forma a não gerar riscos ao negócio;
- Gerenciar acessos (entradas e saídas) e permissões de todos os usuários de acordo com os seus privilégios;
- Realizar monitoramento, testes periódicos e implementação de ações preventivas e corretivas da segurança;
- Criar e validar regras físicas e lógicas de filtragem de dados processados, armazenados ou transmitidos; e

- Verificar se há segurança nos ativos de rede ao serem acessados e ao gerenciarem o tráfego de dados.

A medição dos resultados satisfatórios para o bom andamento do negócio é alcançada respondendo as seguintes perguntas padrões:

- Com qual frequência são realizados testes periódicos de segurança nos diversos ativos da rede corporativa?
- Qual a quantidade de vulnerabilidades descobertas e o número de falhas e brechas abertas no *firewall*?
- Qual a quantidade de sistemas/aplicações que os seus requisitos de segurança não estão sendo atendidos?
- Qual a quantidade de incidentes e problemas que estão prejudicando a reputação interna e externa da empresa? e
- Quantos ataques de violações nas permissões de acesso dos usuários foram feitos no período mensal?

Como auxílio para o bom desempenho do processo Gerenciar Serviços de Segurança, o CobiT 5 dispõem de 7 (sete) práticas chaves para o gerenciamento da segurança e que, conforme a tabela RACI abaixo, define os responsáveis pela execução e pela aprovação de cada uma dessas práticas, bem como, quem deve ser consultado e informado. São elas:

- DSS05.01 - Proteção contra *malware*;
- DSS05.02 - Gerenciamento de segurança da rede e de conectividade;
- DDS05.03 - Gerenciamento segurança *endpoint*;
- DDS05.04 - Gerenciamento de identificação de usuário e acesso lógico;
- DDS05.05 - Gerenciamento de acesso físico para ativos de TI;
- DDS05.06 - Gerenciamento de documentos importantes e dispositivos de saída; e
- DDS05.07 – Monitoramento da infraestrutura para eventos de impacto na segurança.

A Figura 2.10 apresenta a matriz RACI do objetivo DSS05 do CobiT 5 que define todas as partes envolvidas com cada uma das suas práticas chaves de gerenciamento.

DSS05 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS05.01 Protect against malware.						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Manage network and connectivity security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Manage endpoint security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Manage user identity and logical access.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Manage physical access to IT assets.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Manage sensitive documents and output devices.											I					C	C	A			R					
DSS05.07 Monitor the infrastructure for security-related events.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Figura 2.10 - Matriz RACI do objetivo DSS05, CobiT 5. [ISACA (2012)]

Visando o acesso seguro e a utilização correta dos dispositivos móveis dentro da organização, é válido destacar as seguintes práticas chaves, segundo CobiT 5, ISACA (2012):

- DDS05.02 - Gerenciamento de segurança da rede e de conectividade: Usar medidas de segurança e gestão relacionada aos procedimentos/políticas para proteger as informações sobre todos os métodos/meios de conectividade.
    1. Estabelecer e manter uma política de segurança e conectividade;
    2. Permitir somente dispositivos autorizados para ter acesso às informações corporativas e de toda a rede. Definir senhas de acesso;
    3. Implementar filtros de rede (*firewalls*, IPS etc.) para controle do tráfego de rede;

4. Realizar criptografia de dados corporativos conforme sua classificação;
5. Aplicar protocolos de segurança na rede corporativa;
6. Configurar os equipamentos de rede corretamente;
7. Estabelecer mecanismos confiáveis para uma transmissão e uma recepção de dados segura; e
8. Realizar teste períodos de intrusão e de segura dos sistemas.

- DDS05.05 - Gerenciamento de acesso físico para ativos de TI: Definir e implementar procedimentos de concessão, de limite e de revogação ao acesso à instalações, edifícios e áreas corporativas de acordo com as necessidades do negócio, incluindo emergências. O acesso aos locais, edifícios e áreas restritas devem ser justificados, autorizados, registrados e monitorados. Isso deve ser aplicado a todas as pessoas ao entrarem nas instalações, incluindo funcionários, funcionários temporários, clientes, fornecedores, visitantes ou qualquer outro terceiro.
    1. Gerenciar os pedidos e os privilégios de acesso computacional;
    2. Assegurar que os perfis de acessos estão ativos e atualizados;
    3. Monitorar e gerar *log's* de todos os acessos aos *datacenters* e salas de TI;
    4. Instruir a todos os usuários a utilizarem crachá de identificação o tempo todo e em todo lugar;
    5. Exigir que os visitantes sejam acompanhados durante todo o tempo da visita;
    6. Restringir o acesso às áreas sigilosas da TI, criando perímetros de proteção; e
    7. Realizar treinamento regular de conscientização de segurança física.
- DDS05.06 - Gerenciamento de documentos importantes e dispositivos de saída: Estabelecer medidas de segurança físicas adequadas, desenvolvendo práticas seguras por meio de gestão de inventário dos diversos ativos, principalmente dos sigilosos, tais como, formulários especiais, documentos de negociação, documentos impressos para fins especiais e restritos e *tokens* de segurança.
    1. Estabelecer procedimentos para manipulação dos documentos corporativos;
    2. Definir privilégio de acesso aos documentos corporativos;
    3. Criar inventário dos documentos, bem como, ambientes seguros para armazenamento dos dados;

4. Estabelecer medidas de segurança físicas adequadas; e
5. Definir meios seguros de descarte de material corporativo.

Em suma, o objetivo DDS05 fornece toda a estrutura necessária para aplicar e garantir a segurança dos dados corporativos e do ambiente físico da organização. Portanto, suas práticas chaves auxiliarão o Gerente de Segurança a definir e a desenvolver as regras e os procedimentos primordiais para a Política de Segurança da Informação.

Após a fundamentação teórica supramencionada, será iniciado o estudo da metodologia proposta, na qual serão descritos alguns princípios essenciais para implementação de um SGSI e do ciclo PDCA que já é aplicado aos processos do SGSI e neste trabalho proverá um fluxo para implantar um modelo de BYOD em uma corporação.

3 – METODOLOGIA

No corrido mundo dos negócios do século XXI, as organizações tendem a obter vantagem de mercado relevante, em cima dos seus concorrentes, ao proporcionarem, aos seus empregados, facilidades e rapidez no acesso aos seus dados e sistemas corporativos por meio de dispositivos móveis.

A mobilidade dentro das empresas fornece praticidade e melhorias na colaboração entre sócios, empregados e clientes. São documentos, arquivos, *e-mails* e até aplicativos móveis que fazem parte da troca de informações. Tudo isso impulsiona as iniciativas BYOD crescendo de forma exponencial a entrada e o uso dos *smartphones* dentro da organização.

Com isso, cresce a exigência dos empregados na instituição por uma plataforma móvel que ofereça flexibilidade e segurança na transferência de conteúdo corporativo a fim de dar um *upgrade* na produtividade. Logo, surge um novo conceito na *Internet*:

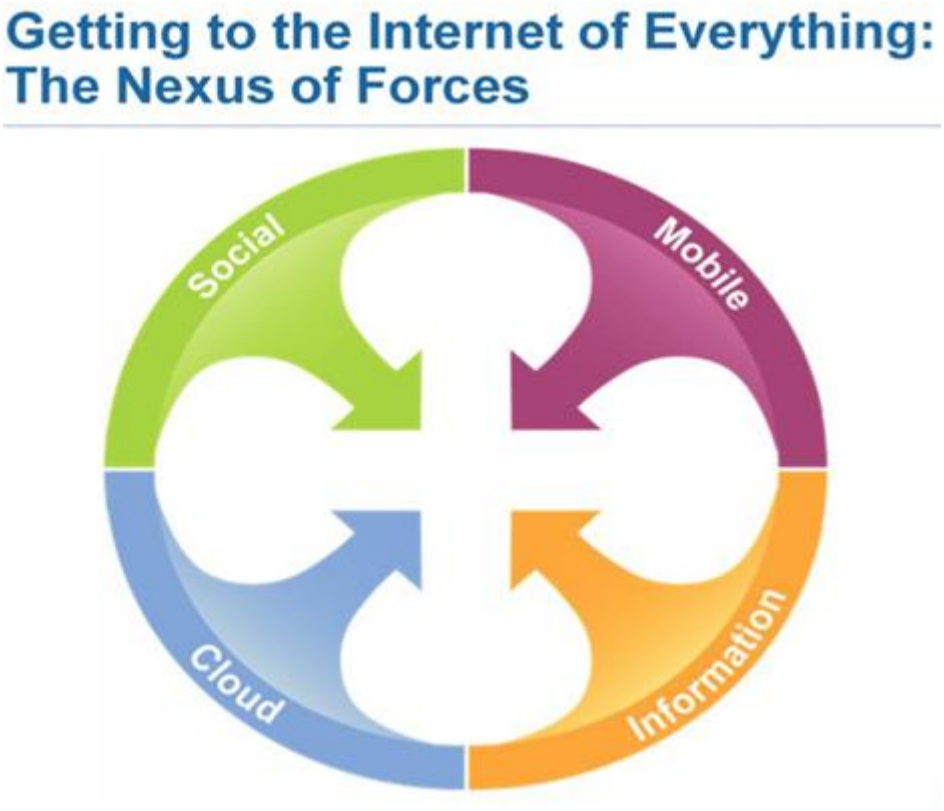

Figura 3.1 - Gartner: The Nexus of Forces. [Things that resonate (2012)]

A Figura 3.1 acima exibe o Nexus das Forças – Obtendo a *Internet* de tudo, conceito criado pela consultoria Gartner Inc. Ela descreve como a convergência e o fortalecimento mútuo de mídias sociais, mobilidade, computação em nuvem e padrões de informação estão criando novas oportunidades de negócios.

Contudo, mesmo com todos os benefícios que a mobilidade tem a oferecer às organizações, soluções de segurança móvel corporativa e políticas de segurança da informação devem ser adotadas e implementadas de forma a proteger as informações e mitigar os riscos no negócio.

Sendo assim, a TI é a principal responsável em gerenciar o fluxo correto e seguro dos dados da corporação, blindando a exposição que o seu negócio sofre com essa nova e prática, porém, vulnerável tendência.

3.1 - SGSI E CICLO PDCA

Um SGSI é projetado para assegurar a seleção de controles de segurança, bem como, fornecer um modelo para a definição, a implementação, a execução, o monitoramento, a revisão, a manutenção corretiva e preventiva e a melhoria da proteção dos ativos de informação.

O SGSI proporciona também uma confiança às partes interessadas com vista a alcançar os objetivos propostos por uma organização, e se baseando numa correta avaliação e gestão dos riscos inerentes ao negócio.

Para se obter a implementação de um SGSI com sucesso, é necessário que a análise dos requisitos esteja voltada para a proteção dos ativos da informação, assim como da garantia dos controles adequados de segurança.

Alguns princípios são essenciais para uma boa implementação do SGSI:

- A atribuição de responsabilidades pela segurança da informação;
- A consciência da necessidade de segurança da informação;
- Avaliar os riscos que determinam os controles adequados para atingir níveis aceitáveis de risco;
- Incorporar o compromisso da gestão e os interesses de todas as partes interessadas;
- Prevenção ativa e detecção de incidentes de segurança da informação;
- Reavaliação contínua da segurança da informação; e

- Reforçar os valores da sociedade.

Com base na segurança da informação, um sistema de gestão facilita com que a empresa:

- Aperfeiçoe os seus planos às atividades;
- Cumpra com os seus objetivos de segurança da informação;
- Faça uma gestão dos seus ativos de informação de uma forma organizada, o que facilita a melhoria contínua; e
- Satisfaça os requisitos de segurança de clientes e outros interessados.

Um processo é a conversão de entradas em saídas e que possui um conjunto de atividades em interação ou em comum. A saída de um processo pode automaticamente dar início a um novo processo, quando isto é realizado de forma bem definida e bem planejada.
A família de Normas ISO 27000:2013 para definição de um SGSI, tem como foco o estudo do princípio adotado nas Normas ISO de Gestão do Sistema, que é conhecido pelo processo PDCA (*Plan – Do – Check – Act*).
Segundo a Norma ISO/IEC 27001:2013:

- PLAN (planejar) – Estabelecer a política, objetivos, processo e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização;
- DO (fazer) – Implementar e operar a política, controles, processos e procedimentos do SGSI;
- CHECK (checar) – Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção; e
- ACT (agir) – Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

A Figura 3.2 demonstra todo o fluxo do modelo PDCA aplicado aos processos do SGSI, desde os requisitos iniciais da segurança da informação até o seu gerenciamento.

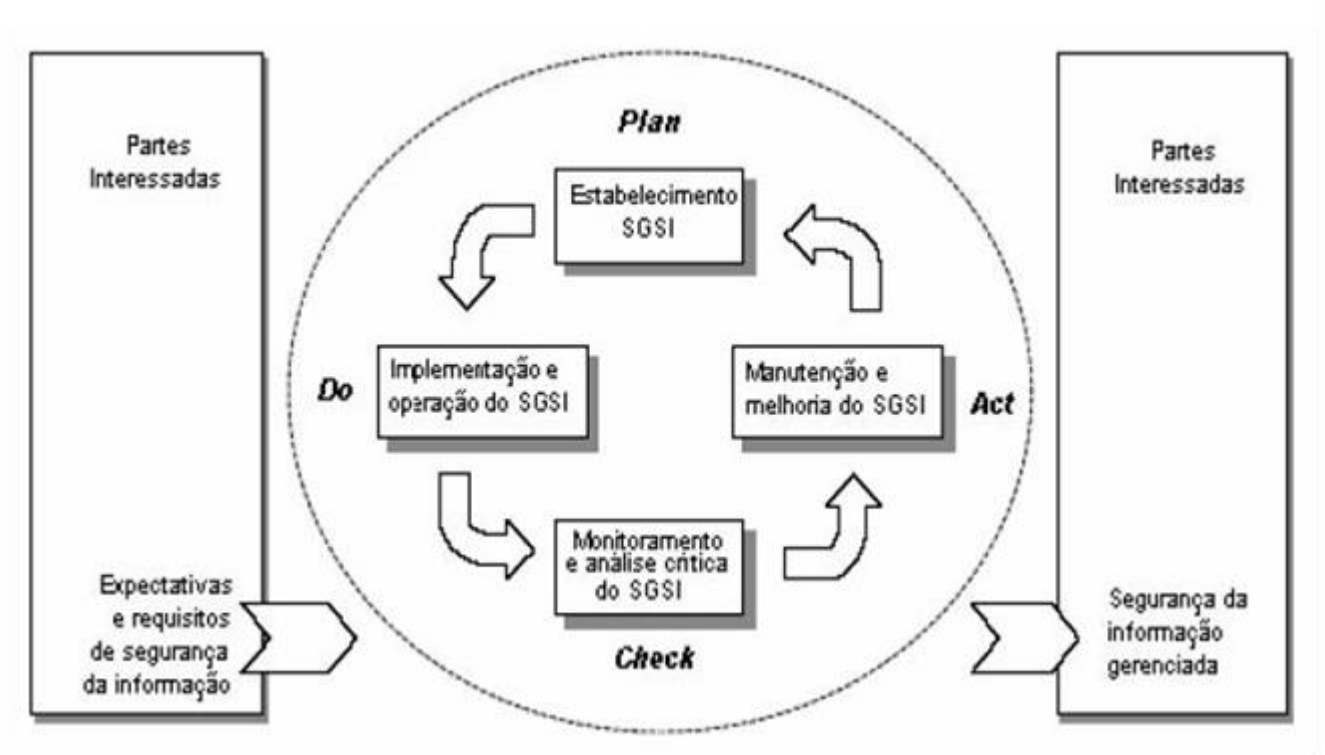

Figura 3.2 - Modelo PDCA aplicado aos processos do SGSI. [Norma ISO/IEC 27001:2013]

A implementação de um SGSI tem como resultado principal a mitigação dos riscos que envolvem a segurança da informação, isto é, reduzir a probabilidade de aparecer incidentes que afetem os ativos de informação e, por conseguinte, diminuindo os demais impactos ao negócio.

Para que o SGSI da organização obtenha a certificação ISO, esta tem de obedecer a um conjunto de requisitos definidos pela Norma ISO/IEC 27001:2013, conforme visto no capítulo anterior deste estudo.

Com base no ciclo PDCA, a próxima seção abordará as principais etapas para implantar um BYOD dentro da corporação.

3.2 - COMO IMPLANTAR UM BYOD

A utilização de BYOD dentro das empresas já se tornou prioridade visto o grande impacto da mobilidade no mundo dos negócios, além disso, já existe um consentimento do uso dessa tendência pelos profissionais de TI. A inserção de aparelhos móveis nas corporações

de todo mundo tem crescido em grande escala, conforme dados abaixo, e isso fez com que surgisse a necessidade de implantação de um programa de BYOD.

Segundo a Gartner Inc., em um dos seus artigos "*Bring Your Own Device: The Facts and the Future.* " (Maio/2013 [dois mil e treze]):

- Existem 1,2 (um vírgula dois) bilhões de trabalhadores móveis em todo o mundo;
- No Japão e nos Estados Unidos, a força de trabalho móvel já representa 75% (setenta e cinco por cento) do total;
- Esses trabalhadores utilizam de 3 (três) a 4 (quatro) dispositivos diferentes para trabalhar; e
- Nesse ritmo, até 2017 (dois mil e dezessete), 50% (cinquenta por cento) das organizações terão programas de BYOD.

Segundo a Ponemon & Symantec em 2013 (dois mil e treze):

- 50% (cinquenta por cento) dos funcionários admite enviar dados da empresa para seu *e-mail* pessoal;
- 41% (quarenta e um por cento) admitiram fazer esse procedimento semanalmente; e
- 37% (trinta e sete por cento) admite usar aplicativos (*apps*) de troca de arquivos (*DropBox*, *GoogleDocs*, *SkyDrive*, etc.) sem autorização do seu empregador.

É relevante ressaltar que esses aplicativos de troca de arquivos mencionados já foram por diversas vezes questionados sobre a segurança dos dados armazenados. Como por exemplo, usuários já tiveram senhas roubadas por *hackers*, arquivos passam a ser controlados também pela empresa que os armazena e problemas de contas liberadas permitindo acesso de qualquer usuário a todos os dados.

Já o cenário das corporações brasileiras ainda é um pouco diferente com relação a adoção de programas de BYOD. Segundo uma pesquisa feita pela empresa Navita entre fevereiro e junho de 2013 (dois e mil e treze), dos 204 líderes de TI que foram ouvidos:

- 9% (nove por cento) afirmam já terem programas implantados e funcionando em suas organizações;
- 32% (trinta e dois por cento) sequer planejam a implantação; e
- Dos 59% (cinquenta e nove por cento) que pretendem adotar a prática, 15% (quinze por cento) planejam fazê-lo ainda em 2013 (dois mil e treze) e 77% (setenta e sete por cento) nos próximos dois anos.

“Significa que, como na maioria dos movimentos tecnológicos, estamos um ano atrás dos Estados Unidos”, afirma Roberto Dariva, CEO da Navita. Segundo ele embora a amostragem de entrevistados seja pequena, ela é representativa, por ter concentrado as entrevistas em grandes empresas, não clientes da empresa, para entender de forma adequada o momento do mercado brasileiro.

A Figura 3.3 mostra mais dados desse estudo, exibe as empresas que já implantaram programas de BYOD (9%) e como está o uso das políticas:

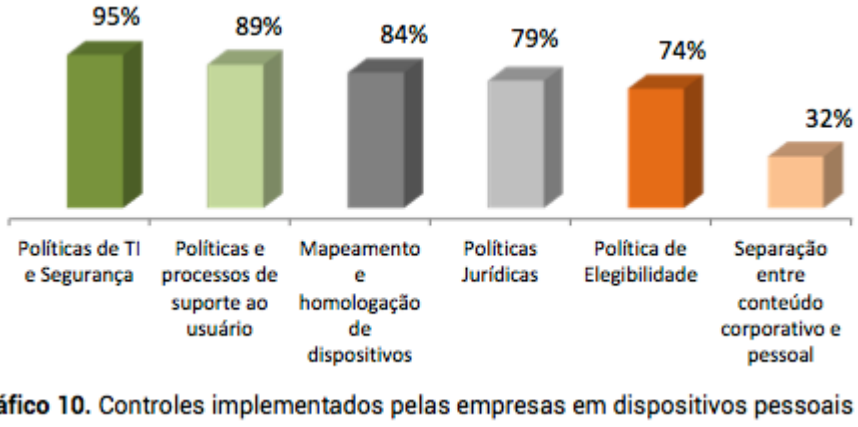

Figura 3.3 - Dados da empresa Navita - programa de BYOD. (CIO NBUSINESS [2015])

Todas essas informações reforçam a importância de implantar uma ferramenta de gerenciamento de conteúdo segura e privada, tendo como base os princípios de um SGSI, do ciclo PDCA e do programa de BYOD.

A seguir serão listadas orientações, tendo como guia a empresa Comstor, de como implantar um programa de BYOD nas corporações e que será utilizado como base deste projeto:

- Realize um mapeamento de todas as metas e os objetivos da corporação. É de extrema importância que o programa de BYOD criado pelo gestor de TI esteja sempre alinhado à área de planejamento estratégico;
- Defina uma Política de Segurança da Informação BYOD para o uso de dispositivos dos empregados. Utilize criptografia, reforce o uso de senhas fortes e adote a utilização de protocolos de segurança para proteção dos dados;

- Faça um levantamento de todos os usuários e de todos os dispositivos, entendendo como eles serão usados na corporação. Pois existem diversos tipos de usuários, aparelhos e áreas de atuação de trabalho:
    1. Existem colaboradores mais avançados tecnologicamente que não precisam de apoio para resolver problemas do aparelho?
    2. Quais colaboradores necessitam ter acesso às informações confidenciais?
    3. Os colaboradores realizam viagens de negócio com frequência? e
    4. Quais são os tipos de aplicativos utilizados pelos colaboradores nos dispositivos?
- Estabeleça quais dispositivos estão autorizados para uso e/ou quais os requisitos mínimos para utilização na corporação. Informe para quais dispositivos a corporação fornece suporte parcial ou total e para quais não fornece nenhum tipo de suporte, além dos aparelhos que já são distribuídos aos colaboradores;
- Determine o responsável pelo suporte dos aparelhos e dos aplicativos. Esclareça, na política BYOD, quem é o responsável pelos aparelhos e quem pagará pelos custos de manutenção;
- Defina o local e a forma de armazenamento dos dados pessoais e corporativos. Por exemplo:
    1. Os dados corporativos serão salvos em um servidor local, nuvem ou em ambos?
    2. Quais serão os critérios utilizados para segmentar e salvar os dados pessoais e os dados corporativos?
    3. Quais aplicativos poderão ser instalados nos dispositivos?
    4. Que tipo e qual tipo de *antivírus*/*antimalware* será usado como padrão nos aparelhos? e
    5. Quais serão os critérios definidos na política BYOD restringindo o acesso às informações sigilosas somente aos colaboradores autorizados?
- Crie regras para casos de demissão e dispositivos perdidos e roubados. Realize um processo de limpeza no dispositivo e suspenda todo e qualquer acesso do colaborador à rede corporativa;
- Utilize sistemas de autenticação. É fundamental que a corporação saiba quem está acessando a sua rede, os seus dados e os seus aplicativos;

- Invista em ferramentas de gestão e gerenciamento de conteúdo. A adoção de uma plataforma de gestão e gerenciamento móvel permitirá à corporação monitorar, supervisionar e gerenciar os dispositivos móveis, as aplicações e os conteúdos; e
- Realize periodicamente treinamentos e capacitações para educar e conscientizar os colaboradores sobre a importância da segurança das informações corporativas, os cuidados necessários para evitar prejuízos à corporação e como utilizar os dispositivos para trazer produtividade para o trabalho.

Logo, as corporações devem se adequar a essa nova realidade que se chama BYOD, adotando medidas que garantam a mobilidade dos colaboradores. A definição de regras e estratégias auxiliará na implantação de uma política BYOD.

Uma boa recomendação é que sejam definidas etapas de implementação do programa, ou seja, realizar testes com um grupo específico de colaboradores ou iniciar com um departamento que utiliza uma quantidade menor de dados sigilos e após isso, estender para os demais departamentos e usuários.

O objetivo da implantação do programa de BYOD vai além da adoção de medidas de colaboração, pois seguindo as etapas do ciclo PDCA e os requisitos de implementação de um SGSI a corporação obterá uma maior confiabilidade para os seus processos e um alto nível de segurança aos dados corporativos.

No próximo capítulo serão apresentadas 4 (quatro) ferramentas de gerenciamento de conteúdo que mais se destacam nesse segmento da área de TI e que possuem como características marcantes a colaboração, a mobilidade e a segurança móvel.

4 - PROPOSTA

A proposta deste projeto visa analisar e apresentar as principais ferramentas de gerenciamento de conteúdo corporativo que oferecem, além de mobilidade, soluções de segurança móvel.

Com isso, definir, com base na fundamentação teórica e na metodologia, uma Política de Segurança da Informação BYOD como guia para as corporações e por fim, realizar a análise dos resultados, ou seja, escolher a melhor ferramenta de gerenciamento de conteúdo dentre as listadas neste trabalho, tendo a teoria estudada como referência.

4.1 - ACCELLION

A Accellion, Inc., é uma das principais organizações mundiais no desenvolvimento de *software* empresarial. Seu foco está em produzir soluções móveis para gerenciar o compartilhamento de arquivos corporativos, aumentando a produtividade dos funcionários e trazendo eficiência e segurança às informações do negócio. A Figura 4.1 exibe a logo dessa organização.

Figura 4.1 - Logo da Accellion, Inc. *All rights reserved*. [Accellion, Inc. (2015)]

Por ser uma das pioneiras na produção de soluções de mobilidade para as empresas, a Accellion ganhou diversos prêmios renomados do mercado empresarial (dentre eles, o prêmio *Gartner* 2014 (dois mil e quatorze) de mobilidade), bem como, publicações em revistas de TI, em reconhecimento da sua liderança e qualidade no desenvolvimento de *softwares*.

Sua fundação foi no ano de 1999 (mil novecentos e noventa e nove) tendo foco inicial no desenvolvimento de tecnologias de *backup* e gerenciamento distribuído de armazenamento de arquivos. Atualmente tem sede na Palo Alto, Califórnia, EUA e está concentrada na criação de soluções móveis que facilitem o compartilhamento, a

transferência e a colaboração segura de arquivos corporativos. A seguir será detalhada a principal solução da Accellion a ferramenta *KITEWORKS*.

4.1.1 - Ferramenta Kiteworks

KITEWORKS (Accellion, Inc.) é uma plataforma de conteúdo para dispositivos móveis que permite compartilhamento e acesso seguro das informações corporativas. Seu objetivo está em aumentar a produtividade do negócio garantindo a segurança e a conformidade dos dados.

Tem como foco os seguintes segmentos do mercado: Organizações de TI, Empresas de Desenvolvimento de *Software* e Instituições Executivas governamentais e não governamentais. Essa ferramenta tem como principais características os seguintes aspectos:

- Ampliar a infraestrutura da organização na utilização de dispositivos móveis: Proporciona uma renovação do parque tecnológico auxiliando no armazenamento e na infraestrutura do conteúdo corporativo no uso dos diversos *smartphones* e *tablets*;
- Criar aplicativos empresariais móveis: permite a criação de fluxos de trabalho, processos e aplicativos corporativos que proporcionam o crescimento da produtividade;
- Fornecer produtividade segura para o negócio: funcionários podem compartilhar, criar e editar conteúdo corporativo de maneira segura em qualquer lugar, utilizando seus dispositivos móveis; e
- Garantir a conformidade e segurança dos dados da organização: garante a proteção do negócio por meio da implantação de nuvem privada, controles de segurança, gerenciamento de conteúdo e geração de relatórios.

A Figura 4.2 detalha algumas das principais características da ferramenta *Kiteworks*, como por exemplo, transferência segura de arquivos, colaboração segura, compartilhamento e acesso seguro e produtividade móvel. Ela exibe também, de forma simples, como é feito o acesso aos dados corporativos pelos dispositivos portáteis na nuvem criada.

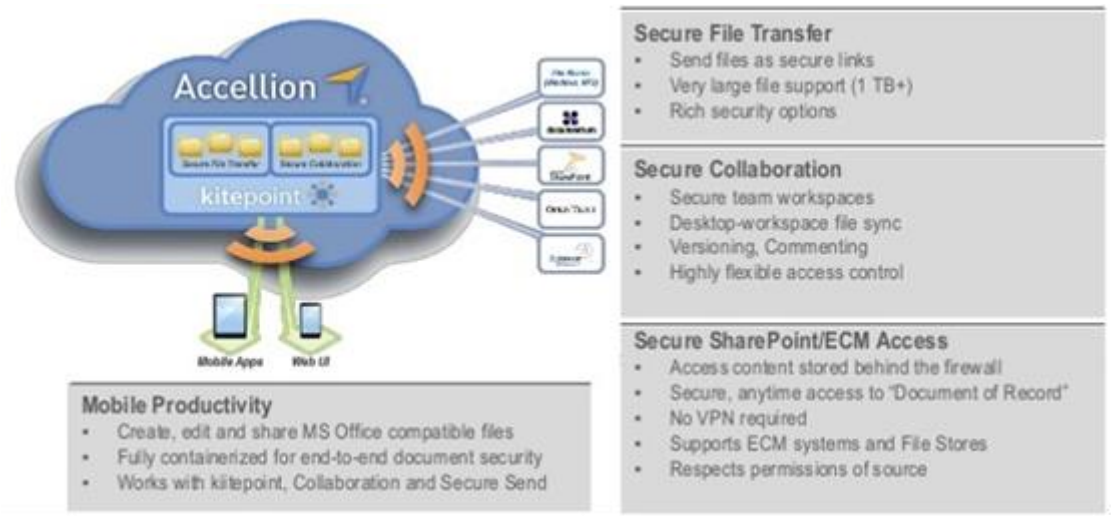

Figura 4.2 - Soluções Accellion – *Kiteworks*. [*blog* Leverage (2013)]

A plataforma de conteúdo *Kiteworks* oferece acesso unificado e seguro para a empresa e para a arquitetura multicamadas da nuvem privada ou híbrida. Dispensa o uso de infraestrutura local para uso da nuvem corporativa ou então configuração no *datacenter* local para garantir a soberania dos dados.

Por possuir acessibilidade universal segura, as organizações conseguem alcançar ganhos de produtividade utilizando mobilidade corporativa do conteúdo, sem gerar riscos de segurança aos dados empresariais.

Diversas são as seguranças obtidas: transferência de arquivos, colaboração do fluxo de trabalho, compartilhamento de dados e produtividade móvel (criação, edição e envio de documentos).

Para a área de desenvolvimento, a *Kiteworks* auxilia na criação rápida de aplicativos móveis inovadores e personalizados que se integram facilmente com as informações empresariais e os sistemas corporativos.

A Figura 4.3 mostra uma das telas da *Kiteworks*, demonstrando o gerenciamento de conteúdo, bem como, a administração do seu *workspaces* e a sua integração com os dispositivos móveis.

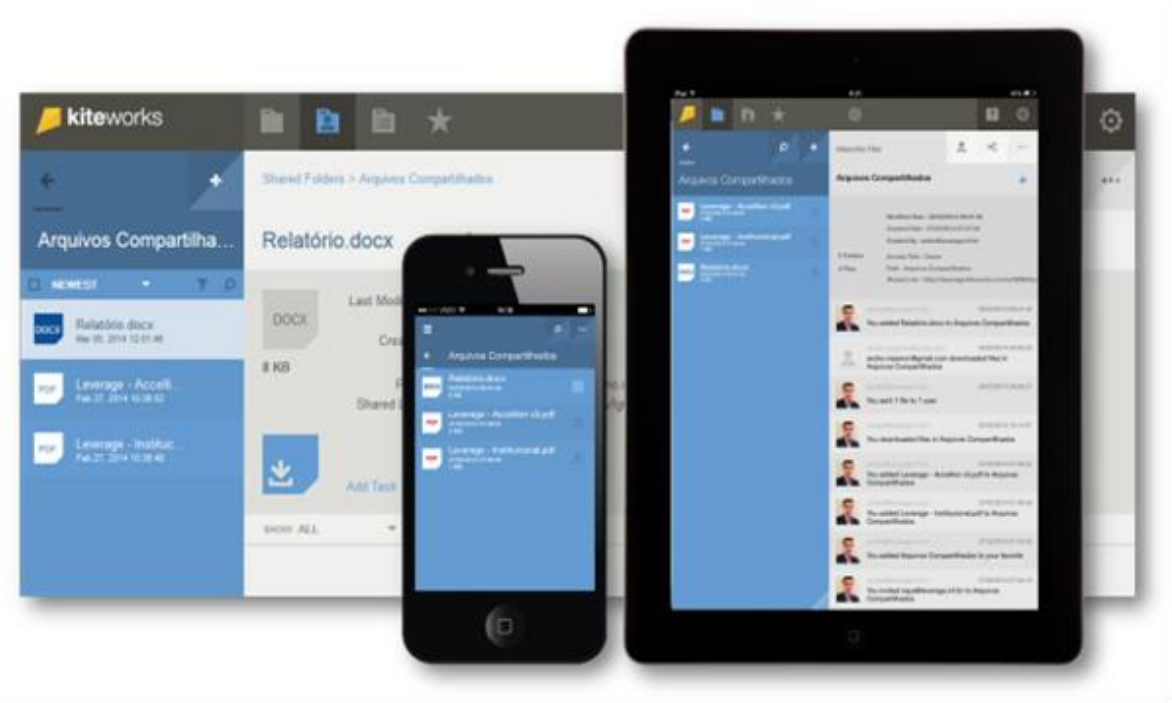

Figura 4.3 - Tela de gerenciamento da *Kiteworks*. [Leverage (2014)]

Com a ferramenta o usuário é capaz de gerenciar os usuários para colaboração, gerenciar arquivos (envio fácil, edição, recebimento etc.), gerar relatórios de atividades, habilitar *plugins* de e-mail e utilizar o *kitedrive* (sincronização de arquivos e nuvem privada corporativa), tudo isso utilizando *smartphones* e *tablets*.

A seguir serão listadas as diversas mobilidades que a ferramenta proporciona para a organização:

- Acesso seguro via SSL (encriptação de dados) sem VPN;
- Aplicativos para os principais dispositivos móveis (iOS, Android e *Windows Phone*);
- Controle de sincronização de *workspaces*;
- Envio de arquivos diretamente do dispositivo ou download daqueles para trabalhar off-line;
- Exportação de arquivos para outras aplicações autorizadas; e

- Plataforma de colaboração segura (compartilhamento, transferência e edição de arquivos, comentários, relatórios e notificações).

A Figura 4.4 apresenta mais uma das funcionalidades da ferramenta *Kiteworks*, demonstrando a praticidade em realizar o envio seguro de arquivos por e-mail.

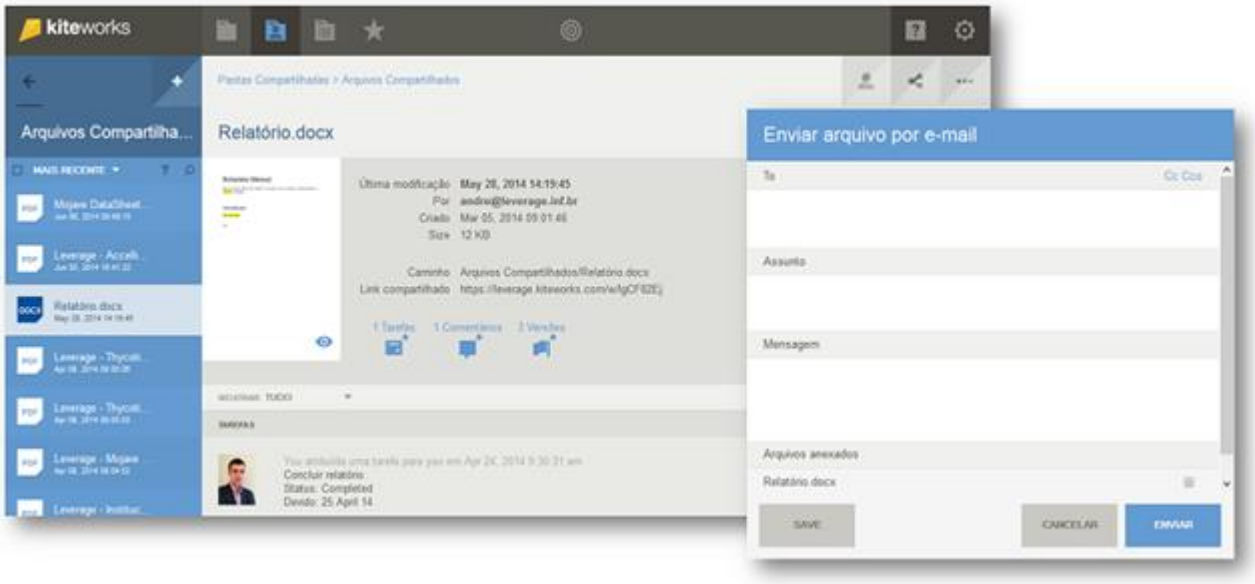

Figura 4.4 - Tela *Kiteworks*. Compartilhamento online de arquivos com segurança. [Leverage (2014)]

Conforme apresenta a Figura 4.5, essa ferramenta possui 4 (quatro) versões sendo todas elas pagas, no entanto, 2 (duas) versões fornecem opções *trial* para teste da plataforma.

	TEAM STARTER	BUSINESS	ENTERPRISE	ENTERPRISE CONNECT
	$75/month	$15/user/month	Custom Pricing	Custom Pricing
	FREE TRIAL	FREE TRIAL	CALL FOR PRICING	CALL FOR PRICING
Features	BUY NOW	BUY NOW		
Users	15 users	5-500 users	Unlimited	Unlimited
File Size Limit	2 GB	2 GB	Unlimited	Unlimited
Storage	500 GB	1 TB	Unlimited	Unlimited
Deployment	Public Cloud	Public Cloud	Private Cloud	Private Cloud

Figura 4.5 - Tabela de preços da ferramenta *Kiteworks*. [Accellion (2015)]

A *Kiteworks* é uma ferramenta móvel pensada no ambiente empresarial, trazendo mobilidade, produtividade e segurança para o negócio. Sendo assim, a Accellion fornece a plataforma ideal para o compartilhamento seguro de informações da empresa, gerando e agregando melhorias significativas, dentre elas, acessibilidade, colaboração, facilidades e controle dos dados para o novo e crescente ambiente móvel corporativo.

4.2 - AIRWATCH BY VMWARE

A *AirWatch* é uma empresa desenvolvedora de soluções empresariais, ela é líder mundial no fornecimento de segurança móvel e no gerenciamento de mobilidade corporativa. A Figura 4.6 exibe a relação dessa empresa com a empresa de virtualização *VMWare*.

Figura 4.6 - Logo *AirWatch by VMWare*. [AirWatch (2015)]

De acordo com dados internos da instituição, mais de 15.000 (quinze mil) organizações em 150 (cento e cinquenta) países utilizam suas plataformas de gerência móvel empresarial para gerenciar o negócio.

Empresa privada com sede em Atlanta, Georgia, a *AirWatch* foi fundada em 2003 (dois mil e três) e sua missão está em desenvolver soluções que forneçam as empresas inovações de tecnologia móvel a fim de revolucionar o modo que as companhias gerem seus negócios.

Em janeiro de 2014 (dois mil e quatorze), por meio de um acordo definitivo, a *VMware* Inc. (líder mundial em infraestrutura em nuvem e em virtualização) adquire a *AirWatch*. E neste mesmo ano pela quarta vez consecutiva, foi reconhecida como líder no Relatório do Quadrante Mágico da *Gartner* pelo gerenciamento de mobilidade empresarial.

Segundo Pat Gelsinger, diretor executivo da *VMware*, a *AirWatch* oferece o melhor e mais seguro gerenciamento móvel corporativo para milhares de empresas em todo o mundo. Com esta aquisição, a *VMware* agregará um elemento fundamental ao nosso

portfólio de computação para o usuário final, que permitirá que os clientes turbinem suas forças de trabalho móveis sem comprometer a segurança.

Sua plataforma de gerenciamento da mobilidade empresarial agrega diversas soluções para gerenciar, por exemplo:

- Aplicativos;
- Conteúdo (dados corporativos);
- Dispositivos móveis;
- *E-mails*;
- *Laptops*; e
- Navegadores.

Cada organização pode implementar as soluções de maneira independente, tendo como base sua política de segurança da informação BYOD. Sua principal ferramenta é o *Secure Content Locker* que fornece uma solução completa para gerenciamento seguro da mobilidade corporativa.

Na subseção a seguir será descrita essa ferramenta que promete inovar a tecnologia móvel e o gerenciamento do negócio das corporações.

4.2.1 - Ferramenta Secure Content Locker

O *Secure Content Locker* (SCL) é uma solução da *AirWatch* que fornece às organizações gerenciamento de conteúdo móvel de forma segura e prática. A Figura 4.7 apresenta a logo dessa ferramenta.

Figura 4.7 - Logo da solução *Secure Content Locker* da *AirWatch*. [ChannelProNetwork (2014)]

Seu foco está em prover um ambiente de acesso ao conteúdo empresarial a todo tempo (*full time*) mantendo os altos níveis de produtividade dentro da empresa.

A proliferação da mobilidade empresarial fez com que a *AirWatch* desenvolvesse uma ferramenta que proporcionasse aos funcionários uma colaboração de conteúdo simples, móvel, segura e universal, mitigando assim os riscos ao negócio.

Essa ferramenta traz diversos benefícios para a organização sendo que os seguintes colaboradores são os que obtêm mais vantagens:

- Administradores de TI: garantem a proteção do conteúdo corporativo, monitoram e controlam o aumento de riscos ao negócio e definem as políticas de uso da ferramenta;
- Executivos: mantêm a força de trabalho móvel produtiva, com atualização dos conteúdos empresariais e com implantação de aplicativos inovadores. Possuem visibilidade total do ambiente da plataforma (dispositivos e usuários) e gerenciam o versionamento de documentos; e
- Usuários finais: acessam o conteúdo corporativo pela ferramenta de múltiplos dispositivos móveis e sistemas operacionais, realizam a colaboração de dados (compartilhamento, envio, edição etc.) a todo tempo e lugar com todos os funcionários cadastrados e são auxiliados pela sincronização bidirecional em dispositivos que a plataforma disponibiliza.

Figura 4.8 - Tela SCL para dispositivos Android. [AirWatch (2015)]

De acordo com a Figura 4.8, a *AirWatch* dispõe de opções flexíveis para o armazenamento do conteúdo empresarial de forma a atender aos requisitos estratégicos da organização. Os dados podem ser hospedados na nuvem pública ou privada (*AirWatch*) sendo facilmente integrada com outras soluções de armazenamento, no datacenter da empresa habilitando acesso seguro sem conexão VPN ou de forma híbrida, ou seja, centralizando e integrando o conteúdo das diversas localidades de hospedagem.
A ferramenta garante segurança de nível empresarial, fornecendo:

- Autenticação *AD/LDAP e Kerberos*;
- Criptografia de dados (AES 256-bit e FIPS 140-2);
- Integração com a solução de Gerenciamento de dispositivos móveis (MDM);
- Listas de controle de acesso e privilégios de permissões;
- Métodos baseados em certificados e *tokens*; e
- Prevenção de perda de dados.

Figura 4.9 - Gerência analítica *realtime* SCL. [VMware | Blogs (2015)]

Por fim, segundo a Figura 4.9, essa solução oferece uma gerência analítica em tempo real do conteúdo por meio de:

- Painéis: no console administrativo a visualização do conteúdo é feita por um inventário (dados detalhados) e o gerenciamento é exibido em tempo real; e

- Relatórios: uma trilha de auditoria completa é feita pela ferramenta, gerando relatórios das atividades dos usuários e dos administradores.

Outras peculiaridades da solução estão relacionadas com a customização da ferramenta, como por exemplo:

- Acesso móvel facilitado (*Android*, *Apple IOS*, *BlackBerry*, *Symbian* e *Windows Phone*);
- Compartilhamento de arquivos por *links* ou pastas;
- Edição de documentos e anotações para versionamento;
- Identidade visual, personalização de temas e CSS;
- Modo de exibição (*View* ou *Collaborate*);
- Opção de implantação flexíveis com outras soluções da empresa;
- Pacote de idiomas para 17 países;
- Portal do usuário para conteúdo pessoal; e
- Sincronização bidirecional de *desktops* (conteúdos em pastas iguais, porém, em *desktops* diferentes são atualizados simultaneamente).

Possui 4 (quatro) versões de gerenciamento cada uma com preços diferenciados, sendo suas licenças por dispositivos ou usuários e a hospedagem nuvem privada da *AirWatch* ou datacenter local da organização. Fornece também outros recursos pagos como adicionais à solução. Conforme dados da Figura 4.10, a ferramenta possui 4 (quatro) versões sendo todas elas pagas, no entanto, 2 (duas) versões fornecem opções *trial* para teste da plataforma.

Figura 4.10 - Tabela de preços SCL, licença por dispositivos. [AirWatch (2015)]

Em síntese, o Gerenciamento de Conteúdo Móvel (SCL) da *AirWatch* permite um acesso móvel seguro, universal e 24x7 (vinte e quatro por sete) ao conteúdo corporativo. Por ser uma solução de compartilhamento e sincronização de dados empresariais, a plataforma fornece também proteção ao conteúdo, mitigando os riscos ao negócio, simplicidade no uso e centralização no acesso ao sistema e geração de relatórios de auditoria.

Logo, o *Secure Content Locker* é uma das soluções ideais e inovadoras para gerir o conteúdo empresarial, trazendo mobilidade, praticidade e segurança para a organização e o negócio.

4.3 – OPENSTACK FOUNDATION

OpenStack Foundation é uma organização sem fins lucrativos responsável pelo desenvolvimento, distribuição e adoção da plataforma *OpenStack*. A organização surgiu em 2012 (dois mil e doze) e possui mais de 9500 (nove mil e quinhentos) membros espalhados em mais de 100 (cem) países. Executivos das principais empresas de TI a nível mundial, como por exemplo, Cisco, HP, IBM, Red Hat, Intel, Dell etc. fazem parte do conselho administrativo da organização. A Figura 4.11 exibe a logo dessa organização.

Figura 4.11 - Logo da empresa *OpenStack Foundation*. [OpenStack (2015)]

O projeto OpenStack surgiu em 2010 (dois mil e dez) de uma parceria entre a Rackspace Inc. (provedor de infraestrutura americano) e a NASA (agência espacial americana). Esta forneceu a sua plataforma Nebula para implementar a parte computacional (*Compute*), ou seja, o módulo de processamento chamado de Nova e aquela a sua plataforma *Cloud Files* para implementar a estrutura de armazenamento de objetos (*Object Storage*), conhecido como *Swift*.

Na subseção abaixo será apresentada essa ferramenta robusta que é baseada em software livre e está voltada para a computação em nuvem.

4.3.1 - Ferramenta OpenStack

OpenStack é um projeto *Open Source* que permite às organizações construírem uma nuvem pública ou privada por meio de uma plataforma de gerenciamento de nuvem. A Figura 4.12 exibe a logo da ferramenta que tem como lema “programação em nuvem”.

Figura 4.12 - Logo da plataforma *OpenStack* - *Cloud Software*. [OpenStack Foundation (2015)]

É considerado também como um sistema operacional para nuvem pois engloba o gerenciamento em larga escala de todos os componentes que envolvem a infraestrutura de TI, como por exemplo, rede, computação, armazenamento etc., fazendo um paralelo com a função que um sistema operacional padrão realiza no *hardware* de uma máquina.

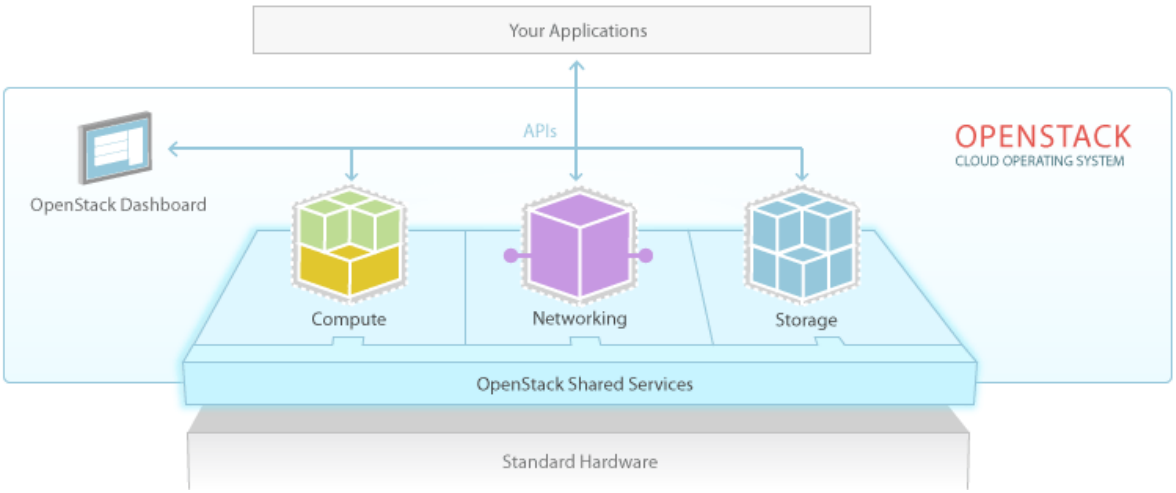

Figura 4.13 - Arquitetura de comunicação da plaforma *OpenStack*. [VMware Brasil 2015]

O *OpenStack* tem como foco a infraestrutura como um serviço e a Figura 4.13 exibe sua arquitetura demonstrando como é feita a comunicação entre cada componente de

infraestrutura que está na nuvem com o *dashboard* da plataforma chegando até as aplicações que utilizam esses recursos.

O projeto *Openstack* foi sendo desenvolvido tendo como característica principal a construção de uma plataforma modular, pois agrupa diversos projetos independentes, proporcionando assim, vários serviços que podem ser implementados em conjunto ou individualmente. A seguir são listados os principais serviços dessa plataforma:

- Block Storage (Cinder) – Módulo de armazenamento em bloco;
- Compute (Nova) – Módulo computacional;
- Dashboard (Horizon) – painel de interação com administradores e usuários;
- Database Service (Trove) – Base de dados de serviços (relacional e não relacional);
- Identity Service (Keystone) – Serviço de autenticação de usuários;
- Image Service (Glance) Serviço para discos e imagens de servidores;
- Networking (Neutron) – Módulo de rede;
- Object Storage (Swift) – Módulo de armazenamento de objetos;
- Orchestration Service (Heat) – Serviço que gerencia múltiplas aplicações de nuvem utilizando *templates*; e
- Telemetry Service (Ceilometer) – Serviço de faturamento dos sistemas por meio de contadores.

4.3.2 - Tecnologia OpenStack Swift

Para este estudo será analisada a tecnologia *OpenStack Swift*, módulo de armazenamento de objetos da ferramenta (*Object Storage*) que tem capacidade de armazenar bilhões de objetos distribuídos por meio de nodos, criando um repositório consistente, provendo gerenciamento e redundância de dados e falhas e realizando streaming e arquivamento de mídia.

Essa plataforma é extremamente escalável suportando uma grande quantidade de objetos de diversos tamanhos (*petabytes*), criando assim, um repositório de dados para máquinas virtuais, aplicações e demais informações corporativas, provendo backups, arquivamento e armazenamento seguro de todos os objetos.

Possui também componentes que realizam o gerenciamento de todos os objetos armazenados na plataforma, são eles:

- Ring;
- Swift Account Server;
- Swift Container Server;
- Swift Object Server; e
- Swift Proxy Server.

A Figura 4.14 mostra as vantagens do módulo *OpenStack Swift* para o armazenamento de grande volume de dados, como por exemplo, diminuição nos custos e compartilhamento de múltiplas aplicações.

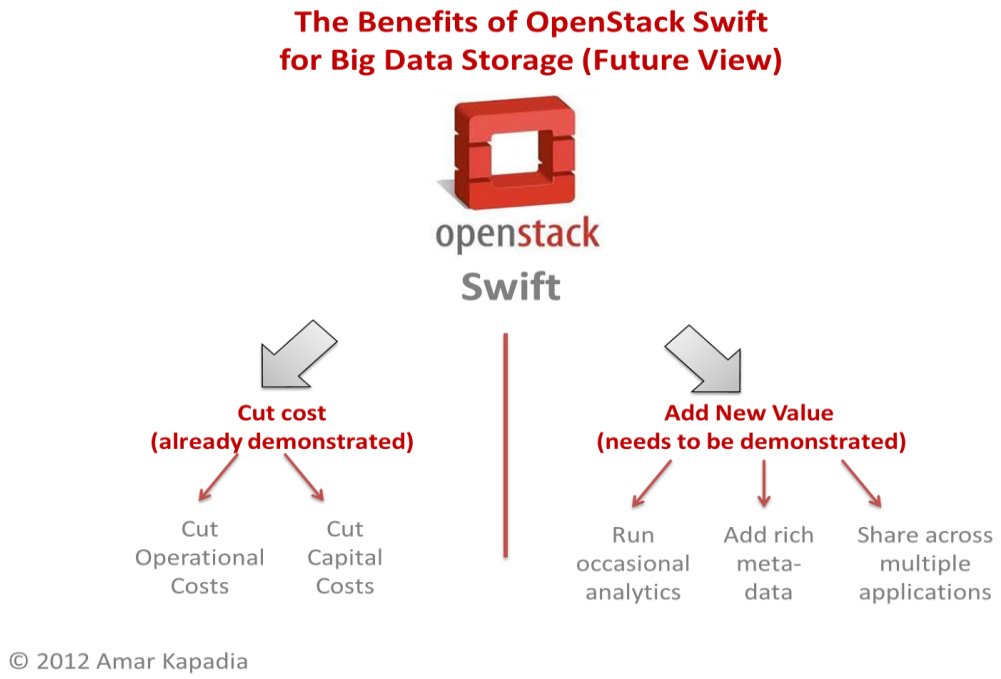

Figura 4.14 - Benefícios do *OpenStack Swift* para armazenamento de grande volume de dados. [Build Cloud Storage (2014)]

Outras vantagens no uso desse módulo são a escalabilidade dos arquivos, ou seja, as informações são replicadas e distribuídas em um *cluster* de milhares de discos, em

servidores distintos, proporcionando assim, um aumento na disponibilidade e durabilidade dos dados.

Existem duas formas para que se tenha uma interface de gerenciamento dos arquivos armazenados entre a plataforma e o usuário, e a primeira delas é agregar ao módulo Swift uma API (*Application Program Interface*), ou seja, por meio de *scripts* desenvolver uma interface para manipular os dados, realizando assim a colaboração das informações (alterar, atualizar, baixar, copiar, criar, deletar, editar, exibir, listar e remover arquivos).

Já a segunda solução é utilizar clientes GUI (*Graphical User Interface*) criada por desenvolvedores para realizar a interação e o compartilhamento de informações da ferramenta com os colaboradores. Várias soluções são pagas, como por exemplo, o *Gladient Cloud Desktop* e o *Cloudberry Explorer* e dentre as opções *Open Source* destaca-se o *Cyberduck*.

4.3.3 – Projeto Manila

Outra solução da plataforma *OpenStack* é o projeto Manila que ainda está em desenvolvimento pela *OpenStack Foundation*. Esse módulo fornecerá um sistema dedicado e exclusivo de arquivos compartilhados como um serviço.

A seguir são listadas as principais características e funcionalidades que esse módulo proporcionará:

- Acesso simultâneo à múltiplos dados;
- Alta disponibilidade de dados;
- Armazenamento baseado em arquivos compartilhados;
- Arquitetura baseada em componentes;
- Compatibilidade com diversas API's;
- Mapeamento de sistemas de armazenamento externo (NAS/NFS/SMB);
- Provisionamento automatizado de compartilhamentos de arquivos;
- Recuperação e tolerância à falhas e perda de dados; e
- Segurança com lista de controle de acesso (ACL) e com protocolo LDAP.

O módulo Manila está disponível no momento apenas para testes e seus usuários podem experimentar seus recursos e assim, analisar como eles podem se adequar ao

ambiente corporativo, contudo, assim que estiver totalmente desenvolvido, proporcionará confiabilidade, economicidade, escalabilidade e segurança às informações corporativas

Em suma, *OpenStack* é a forma mais robusta, prática, estruturada e segura *OpenSource* para armazenar informações, sincronizar dados, gerenciar tarefas e conteúdo corporativo e compartilhar arquivos fornecendo mobilidade e proteção ao negócio.

4.4 - EYEOS

A EYEOS é um projeto de código aberto na Europa, sua solução possui mais de 1 (um) milhão de *downloads* e comunidades espalhadas no mundo inteiro. A Figura 4.15 mostra a logo desse projeto, bem como, seu lema: " soluções para um novo mundo. ".

Figura 4.15 - Logo do projeto EYEOS - *Solutions for a new world*. [EyeOS S.L. (2012)]

O projeto teve início em 2007 (dois mil e sete) com um pequeno grupo de desenvolvedores na cidade de Barcelona - Espanha. A equipe utilizou conhecimentos de linguagens de programação *web* (HTML, PHP, AJAX e JavaScript) para prover um ambiente de área de trabalho *web*, dinâmico e com mobilidade.

Seu projeto é utilizado e patrocinado por várias empresas mundiais e possui diversos prêmios na área de TI. Como prêmio destaque ganhou o Gartner em 2011 (dois mil e onze) que selecionou o EyeOS como um dos 5 (cinco) melhores fornecedores em Gestão de Operações de TI.

Na subseção abaixo será analisada as principais características e funcionalidades da ferramenta EyeOS.

4.4.1 - Ferramenta EyeOS Professional Edition

A ferramenta EyeOS é um sistema multiplataforma desenvolvido para ambientes corporativos e sua estrutura é baseada nos conceitos de *cloud computing*. Ela possui licença GPL, sendo seu código aberto e gratuito.

O EyeOS proporciona para os seus usuários um novo conceito de gestão de *desktop*. Chamado também de *cloud desktop*, o EyeOS fornece, a partir da nuvem, uma área de trabalho com ferramentas de gestão de informações pessoais, de colaboração e de gerenciamento de arquivos.
A ferramenta tem como pilar 3 (três) principais benefícios:

1. Aumentar a produtividade por meio de ferramentas de colaboração;
2. Melhorar a mobilidade dos funcionários proporcionando acesso por vários dispositivos e em qualquer lugar; e
3. Reduzir custos de gerenciamento de áreas de trabalho por meio de virtualização.

Seus recursos proporcionam uma dimensão social da plataforma e a facilidade de realizar virtualização de *desktops* híbridos. A Figura 4.16 apresenta a área de trabalho social dessa solução, demonstrando a praticidade no acesso feito em navegadores, um dos tipos de segurança para *web* utilizados, os certificados *SSL* e alguns dos diversos aplicativos que a ferramenta disponibiliza por padrão aos seus usuários.

Figura 4.16 - Área de trabalho social da ferramenta EyeOS. [EyeOS S.L. (2012)]

Segundo o site do EyeOS, a ferramenta é uma solução projetada para o Departamento de TI, pois se encaixa perfeitamente entre a infraestrutura e as camadas de aplicação. O EyeOS é executado em servidores da corporação criando uma nuvem privada que é acessada pelos *desktops* clientes via *browser*.

Possui uma arquitetura de cluster e contém um *framework* para garantir segurança às operações. No entanto, sua filosofia de segurança recomenda que seja configurado na empresa uma boa política de segurança como padrão.

A ferramenta fornece diversas vantagens para a área de TI das empresas, por exemplo:

- Armazenamento de dados por: *file system* e metadados;
- Aumento de desempenho operacional com virtualização híbrida e em HTML5;
- Conectividade simples com a infraestrutura corporativa;
- Fácil integração com as aplicações e sistemas da corporação;
- Ganhos em escalabilidade horizontal e disponibilidade com arquitetura clusterizada;
- Personalização da ferramenta e desenvolvimento de aplicativos móveis; e
- Segurança baseada em defesa de profundidade por *host*, separação de funções e visualizador de *logs*, sendo a dependência da solução somente corporativa e a garantia da confiabilidade por meio de certificados *SSL*.

Figura 4.17 - Solução EyeOS nos diversos dispositivos móveis. [EyeOS S.L. (2012)]

A Figura 4.17 exibe a interface da solução EyeOS nos variados dispositivos portáteis do mercado, demonstrando a sua fácil e prática integração e comunicação.

Logo, o EyeOS *Professional Edition* é uma plataforma voltada para a mobilidade corporativa que oferece *desktops web*, ambiente de produção em nuvem privada, ferramentas de colaboração e segurança móvel. A solução é gratuita, porém, as empresas devem entrar em contato com o canal de vendas para obter mais informações de como adquirir a ferramenta.

4.5 - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO BYOD

O crescente avanço da TI e das suas tecnologias proporciona não somente melhorias ao negócio das organizações, mas também, aos seus funcionários que começam a utilizar dispositivos móveis pessoais para realizar as diversas tarefas atribuídas no ambiente de trabalho.

O contexto exposto é a definição para consumerização da TI, ou seja, *smartphones*, *tablets*, *ultrabooks* etc., começam a fazer parte da rotina do expediente dos colaboradores por já estarem inseridos no seu dia a dia, promovendo assim, o aumento da produtividade por meio da mobilidade e da praticidade.

Por outro lado, a utilização dessa nova prática favorece o surgimento de alguns riscos ao negócio, podendo prejudicar a relação da empresa no competitivo mercado externo. Esse fato ocorre pois não existe ainda um controle e uma gestão pelo Departamento de TI das organizações dos vários dispositivos móveis que entram e saem diariamente das instalações das instituições.

Não existem ainda medidas de segurança adequadas para combater invasões, ataques e infecções causadas por *malwares* ou roubo de dispositivos. Logo, brechas na segurança móvel se tornam mais comum, bem como, perda de dados armazenados nesses aparelhos por roubo ou captura são mais frequentes e aplicações e falta de atualização podem gerar um aumento de incidentes e vulnerabilidades.

Contudo, todo esse cenário faz com que cresça a necessidade da análise de viabilidade para implementação de uma Política de Segurança da Informação que contemple o novo movimento das empresas o chamado BYOD (*Bring Your Own Device*) – traga seu próprio dispositivo móvel.

Um passo importante para as empresas gerirem a consumerização da TI é adotar e desenvolver uma estratégia bem definida para interação dos diversos dispositivos móveis, focar esforços na proteção da rede corporativa e incentivar a colaboração segura entre todas as áreas e funcionários da instituição.

A Política de Segurança da Informação para dispositivos BYOD é uma maneira da organização e do Gerente de TI se resguardarem caso algum funcionário faça um uso indevido de suas permissões, infringindo as regras e medidas propostas. A política deve definir os critérios de aceitação para uso dos dispositivos móveis no ambiente corporativo.

É importante que essa documentação seja completa, abrangendo todos os pontos que se referem à mobilidade e segurança, porém, seja de fácil entendimento e acesso por todas na empresa. Como forma de validação e aplicação das novas regras de uso de aparelhos móveis, é necessário que cada um dos funcionários, ao tomar conhecimento da política, assinem um termo de ciência da mesma e de comprometimento em cumpri-la.

Etapas iniciais e necessárias para implementação de uma política de segurança que devem ser analisadas, avaliadas e definidas pela alta direção e o Gerente de TI:

- Atribuição formal das penalidades/punições e das responsabilidades de uso incorreto do BYOD;
- Classificação de todos os dados e informações da empresa;
- Definição das instruções e processos de trabalho;
- Escolha das tecnologias mais eficientes para prover segurança; e
- Realização constante de capacitações, treinamentos e conscientização de uso da política.

O passo seguinte é a definição da política que deve estar alinhada às estratégias do negócio, bem como, às normas e guias já listados em capítulos anteriores deste projeto. As regras e os critérios da documentação devem ter como base a seguinte estrutura:

1. Objetivo da política BYOD;
2. Abrangência do programa BYOD;
3. Definição dos requisitos de segurança à serem cumpridos;
4. Permissões de acesso e uso BYOD; e
5. Termos e referências jurídicas.

A seguir serão listadas definições e regras para uma boa e eficaz Política BYOD baseada na Política de Segurança da Informação – ANEXO I – BYOD da Universidade Veiga de Almeida, Rio de Janeiro:

1. Dispositivo móvel é qualquer equipamento que possa ser transportado e utilizado em ambiente externo aos limites físicos da organização;
2. Recurso exclusivo da organização é qualquer serviço oferecido aos colaboradores para o exercício de sua atividade profissional (e-mail, sistemas, servidores, rede etc.);
3. Os sistemas operacionais permitidos para BYOD são *Android* (Google) iOs (*Apple*) e *Windows Phone*;
4. A área de TI é responsável pela gestão dos dispositivos móveis BYOD na organização, que consiste em atividades de monitoramento e controle;
5. Todo dispositivo móvel BYOD está sujeito ao controle da TI, sendo monitorado os seguintes pontos:
    a) Informações técnicas dos dispositivos e versões de software;
    b) Configurações de segurança;
    c) Histórico de instalação de aplicativos;
    d) Localização geográfica; e
    e) Espaço físico disponível (disco) e capacidade da bateria.
6. Funções que a TI tem capacidade de executar:
    a) Bloquear remotamente o dispositivo;
    b) Apagar todos os dados do dispositivo;
    c) Instalar um aplicativo remotamente; e
    d) Alterar a configuração da política de segurança do aparelho.
7. Todo colaborador deve procurar a TI para solicitar autorização e configurar o BYOD em seu dispositivo para acesso aos recursos da organização;
8. Em caso de problemas e perdas do dispositivo, a TI deve ser informada para tomar as devidas providências de segurança (bloqueio e limpeza de dados do aparelho); e
9. Toda e qualquer utilização indevida dos dispositivos móveis está sujeito às regras previstas na política, sofrendo as devidas penalidades e punições.

Por fim, deve-se iniciar pela área de TI a execução do plano BYOD, ou seja, realizar a formalização e a divulgação da política de uso, definir os períodos de

treinamento e de capacitação e prover a aquisição e a instalação das tecnologias necessárias de segurança e gestão dos processos BYOD. Como fator de sucesso dessa medida é viável realizar auditorias internas, bem como, atualizar e corrigir periodicamente a política.

Em síntese, a Política de Segurança da Informação BYOD é de extrema importância para que as organizações estabeleçam os meios e as condições para que seus colaboradores utilizem seus dispositivos móveis no ambiente empresarial sem comprometer os dados corporativos, fornecendo proteção ao negócio e segurança à mobilidade.

Na última seção deste capítulo serão analisados os resultados da comparação entre as ferramentas e as normas e os guias estudados para definição da melhor solução de gerenciamento de conteúdo que oferecerá maior mobilidade corporativa e segurança ao negócio das corporações.

4.6 - ANÁLISE DOS RESULTADOS

Nesta seção, serão apresentados os resultados deste projeto. Inicialmente, será apresentado uma tabela relacionando as áreas de segurança das bibliotecas e normas estudadas, uma segunda tabela listando os graus de prioridade para avaliação das ferramentas e, por fim, uma terceira tabela que com base na primeira informará qual a melhor ferramenta de gerenciamento de conteúdo, dentre as estudas, para se implantar em uma corporação.

Tabela 4.1 - Comparativo das áreas de Segurança da Informação - ISO/IEC 27001:2013, ISO/IEC 27002:2013, CobiT 5 e ITIL v3.

TECNOLOGIA DA INFORMAÇÃO					
SEGURANÇA DA INFORMAÇÃO					
GESTÃO DE SI	**GESTÃO DE SI**	**GOVERNANÇA DE TI**		**GESTÃO DE TI**	
ISO/IEC 27001	**ISO/IEC 27002**	**COBIT 5**		**ITIL v3**	
Modelo para um SGSI	Código de boas práticas para GSI	PROCESSO	OBJETIVOS	PROCESSO	OBJETIVOS
Definição de um	**Definição de**	**DDS05 -**	DSS05.01 -	**Gerenciamento**	Confidencialidade

SGSI Responsabilidades da alta direção Auditorias internas para validar o SGSI Análise crítica do SGSI Melhoria contínua do SGSI	**uma Política de Segurança da Informação** Guiar a alta direção com relação à segurança da informação **Divulgação da política/fácil acesso e entendimento** Revisão e melhoria contínua	**Gerenciamento de serviços de segurança**	Proteção contra *malware*; **DSS05.02 - Gerenciamento de segurança da rede e de conectividade;** DDS05.03 - Gerenciamento segurança *endpoint*; DDS05.04 - Gerenciamento de identificação de usuário e acesso lógico; **DDS05.05 - Gerenciamento de acesso físico para ativos de TI;** **DDS05.06 - Gerenciamento de documentos importantes e dispositivos de saída;** e	**da Segurança da Informação**	dos dados Integridade dos dados Disponibilidade dos dados Autenticidade **Política de Segurança da Informação** **Gerente de Segurança**
Estrutura para gerenciar a segurança de TI: **Controlar** **Planejar** **Implantar** **Avaliar** **Manter**					

			DDS05.07 – Monitoramento da infraestrutura para eventos de impacto na segurança.		

A Tabela 4.1 mostra um comparativo das áreas de Segurança da Informação que fazem parte dos principais segmentos da área de TI, a governança e a gestão. São destacados também os pontos em comum entre as Normas e as bibliotecas.

Com os dados levantados fica fácil compreender que elas estão bem relacionadas e que a aplicação conjunta trará um nível elevado de excelência na aplicação da Segurança da Informação na corporação.

A próxima tabela auxiliará na escolha das ferramentas estudadas, pois nela serão descritos os critérios para pontuação de cada um dos seus requisitos técnicos e funcionais.

As ferramentas de gerenciamento de conteúdo serão classificadas e pontuadas de 0 (zero) a 5 (cinco) conforme suas funcionalidades. Será atribuído um grau de prioridade a cada um dos requisitos.

A Tabela 4.2 define o sistema de classificação para os requisitos que serão atribuídos durante a avaliação:

Tabela 4.2 - Descrição dos graus de prioridade utilizados para avaliação das ferramentas.

CLASSIFICAÇÃO DO INDICADOR	GRAU DE PRIORIDADE	DESCRIÇÃO
Inexistente	0	A ferramenta não contempla o requisito.
Muito ruim	1	Poderá existir uma forma de adaptação da ferramenta ao requisito.
Ruim	2	Existe uma forma de adaptação da ferramenta ao requisito.
Regular	3	A ferramenta apenas contempla o requisito

		parcialmente.
Bom	4	A ferramenta contempla o requisito.
Excelente	5	A ferramenta excede o requisito.

A Tabela 4.3 estará listando as ferramentas de gerenciamento de conteúdo estudas, relacionando-as com os principais pontos da primeira tabela e, também, com os requisitos necessários para adequá-las ao programa de BYOD sugerido.

Neste quadro comparativo serão analisados 17 (dezessete) requisitos técnicos e funcionais essências para uma ferramenta de gerenciamento de conteúdo. Esses pontos são a fase final para que uma corporação possa escolher a ferramenta que melhor se adeque e atenda o seu negócio de TI.

A seguir são listados os requisitos levantados:

- Acesso unificado (*on demand*) e seguro das informações;
- Armazenamento dos dados;
- Colaboração do fluxo de trabalho;
- Compartilhamento seguro das informações;
- Conformidade dos dados;
- Criação de aplicativos móveis;
- Disponibilidade para as principais plataformas móveis;
- Gerência analítica *realtime*;
- Licença gratuita;
- Métodos de segurança;
- Mobilidade corporativa do conteúdo;
- Nuvem privada ou híbrida;
- Prevenção de perda de dados;
- Produtividade móvel;
- Sincronização de dados bidirecional;
- Solução de *backup*; e
- Virtualização híbrida e clusterização.

Os requisitos destacados em vermelho são aqueles que estão relacionados com a primeira tabela e, sendo assim, são considerados como os mais importantes para informar o nível de segurança da informação que uma ferramenta pode prover.

Tabela 4.3 - Comparativo das ferramentas de gerenciamento de conteúdo.

	KITEWORKS	SECURE CONTENT LOCKER	OPENSTACK	EYEOS
Acesso unificado (*on demand*) e seguro das informações	5	5	5	5
Armazenamento dos dados	4	4	4	5
Colaboração do fluxo de trabalho	5	5	5	4
Compartilhamento seguro das informações	4	5	5	4
Conformidade dos dados	5	4	4	4
Criação de aplicativos móveis	4	3	4	5
Disponibilidade para as principais plataformas móveis	3	4	4	4
Gerência analítica *realtime*	4	5	4	3
Licença gratuita	0	0	5	4
Métodos de segurança	4	5	5	5
Mobilidade corporativa do conteúdo	5	5	5	5

Nuvem privada ou híbrida	4	5	5	3
Prevenção de perda de dados	3	5	4	1
Produtividade móvel	5	5	5	5
Sincronização de dados bidirecional	4	4	3	3
Solução de *backup*	3	3	4	3
Virtualização híbrida e clusterização	3	3	4	5
PONTUAÇÃO FINAL	**65**	**70**	**75**	**68**

É importante destacar que para a escolha de uma ferramenta de TI, é necessário definir quais informações devem ser extraídas do *software*, pois diversas opções com inúmeras funcionalidades podem ser encontradas no mercado. No entanto, a aquisição ideal sempre será aquela solução que se adequa e se adapta conforme as necessidades da corporação e que proporciona também um melhor custo benefício.

Com a pontuação final do quadro comparativo das ferramentas de gerenciamento de conteúdo pode-se verificar que a ferramenta *OpenStack* obteve a maior pontuação dentre as 4 (quatro) soluções estudadas. Ela demonstra ser uma solução bem robusta, com muitas funcionalidades que atendem as diversas necessidades de uma corporação na área de TI e fornece qualidade e segurança para o gerenciamento de conteúdo corporativo.

Porém, assim como a plataforma *OpenStack*, a ferramenta *Secure Content Locker* foi a solução que obteve melhor pontuação nos requisitos técnicos e funcionais definidos como primordiais (requisitos destacados em vermelho) para prover qualidade, eficiência, segurança, mobilidade e produtividade móvel para o compartilhamento das informações corporativas.

Em suma, a escolha da ferramenta deve ser avaliada pelo Gerente de Segurança da área de TI da corporação levando em consideração o planejamento estratégico traçado para o negócio da mesma.

Por fim, as ferramentas estudadas oferecem grandes recursos para que a área de TI venha a gerenciar da melhor forma possível e com segurança as informações corporativas, auxiliando assim, para que o programa de BYOD seja eficaz e eficiente em todos os níveis hierárquicos da corporação.

5 - CONCLUSÕES

No século XXI, a Tecnologia da Informação está atuando como protagonista no mundo corporativo fornecendo métodos e soluções em diversas áreas, como por exemplo, desenvolvimento, infraestrutura, telefonia, redes de comunicação etc. Todo esse avanço está proporcionando também praticidade e muitos benefícios a todos que a aderem. Um exemplo disso é o surgimento dos dispositivos móveis ou portáteis que vieram para agregar e revolucionar a forma como as pessoas interagem e se comunicam ao redor do mundo.

Esse cenário fez surgir dentro das corporações a consumerização da TI, ou seja, a forma de unir esses dispositivos pessoais com as suas soluções de trabalho, trazendo colaboração e mobilidade. No entanto, um dilema aparece à área de TI: “ como prover segurança ao negócio TI? ”, tal fator está fazendo com que ela busque novos meios de proteger todo o ambiente e a rede corporativa.

Neste projeto foi apresentado, por meio de algumas pesquisas, a falta de conhecimento e estrutura das corporações para implantar um programa de BYOD e como a sua implementação traz melhorias significativas por meio da segurança. Como por exemplo, adotar e aplicar políticas de segurança adequadas, estipular regras e conscientizar todos os colaboradores sobre os riscos do mau uso de seus equipamentos no ambiente corporativo são algumas das medidas preventivas contra vazamento de informações que envolvem o negócio.

A pesquisa bibliográfica realizada proporcionou conhecer e compreender o que as Normas, bibliotecas e *frameworks* de TI de nível mundial abordam sobre os mecanismos necessários para inserir a segurança da informação na corporação. Esses conceitos foram essências para definir qual a melhor solução para gerir de forma segura os dados corporativos.

Foi visto também neste estudo, as principais ferramentas de gerenciamento de conteúdo corporativo, apresentando suas funcionalidades, características, praticidades, benefícios e como elas fornecem às corporações mobilidade, comunicação, colaboração e compartilhamento seguro de informações.

Por fim, por meio de tabelas, foram exibidos os dados mais relevantes para montar os quadros comparativos propostos a fim de relacionar o que tem de mais importante na área de segurança da informação da fundamentação teórica estudada, propor graus de

prioridade para realizar uma avaliação das soluções analisadas e, assim, escolher qual a melhor ferramenta de gerenciamento de conteúdo corporativo para adotar em uma corporação. Como já foi orientado, toda essa escolha deve ser feita tendo como base o tipo de negócio e as estratégias de TI da corporação.

Em suma, por meio da aplicação de conceitos teóricos e ferramentas de segurança da informação adequadas pode-se tornar o ambiente corporativo propício a receber um programa BYOD. As corporações estão cada vez mais evoluindo para aderir à mobilidade, porém, elas precisam encontrar meios adequados para incorporá-las à consumerização de TI, de forma a tornar o seu ambiente de produção com nível de segurança apropriado sem pôr em risco a continuidade do negócio, mas trazendo qualidade e eficiência para as tomadas de decisão.

5.1 - TRABALHOS FUTUROS

A mobilidade proporciona às corporações novas maneiras de ampliarem e maximizarem seus lucros e de se tornarem cada vez mais um diferencial no competitivo mundo dos negócios. Fornece caminhos inovadores a todos os seus *stakeholders*, facilitando a integração e a colaboração e promovendo um ambiente mais produtivo e com qualidade.

A aquisição de uma solução de gerenciamento de conteúdo deve estar sempre adequada às estratégias de negócio da corporação e ao programa de BYOD. Sendo assim, serão listadas propostas para trabalhos futuros que enriquecerão este projeto e que trarão às corporações novos mecanismos para prover excelência ao seu negócio pela gestão e a governança de TI. Abaixo são apresentadas essas propostas:

- Adequar à política BYOD regras e procedimentos de autointegração dos dispositivos trazidos pelos colaboradores à corporação;
- Adotar a metodologia de gerenciamento de projetos PMBoK para condução na implantação das Normas, das bibliotecas e das ferramentas estudadas;
- Integrar as ferramentas de gerenciamento de conteúdo com BI para prover mais segurança e uma melhor tomada de decisão;
- Introduzir na política BYOD as formas de treinamento e capacitação de todos os colaboradores; e
- Seguir a IN MP/SLTI N° 04 para obter qualidade e melhores orientações na contratação de soluções de TI.

REFERÊNCIAS BIBLIOGRÁFICAS

ACCELLION INC. (2015) **Site oficial**. Disponível em: http://www.accellion.com/ > Acesso em: 15 jun. 2014.

AIRWATCH BY VMWARE (2015). **Site oficial da *AirWatch***. Disponível em: http://www.air-watch.com/ > Acesso em: 22 nov. 2014.

ALCA SYSTEM TELECOMUNICAÇÕES (2014). **Como garantir segurança dos dispositivos móveis na empresa**. Disponível em: http://www.alcasystem.com.br/como-garantir-seguranca-dos-dispositivos-moveis-na-empresa/ > Acesso em: 16 out. 2014.

ASHFORD GLOBAL INFORMATION TECHNOLOGY (2014). **Entendendo os 4 Ps do ITIL v**3. Disponível em: http://www.ashfordglobalit.com/training-blog/itil-tips-and-training/understanding-the-four-ps-of-itil-service-management.html > Acesso em: 17 dez. 2014.

ASUG BRASIL (2014). **Brasil segue sem política de segurança para BYOD**. Disponível em: http://www.asug.com.br/brasil-segue-sem-politica-de-seguranca-para-byod/ > Acesso em: 12 jan. 2015.

BLOG LEVERAGE (2013). **Proteção de dados em dispositivos móveis**. Disponível em: http://blog.leverage.inf.br/2013/11/07/protecao-de-dados-em-dispositivos-moveis/ > Acesso em: 20 jun. 2014.

BUILD CLOUD STORAGE (2014). ***The Significance of Hadoop running on OpenStack Swift***. Disponível em: http://www.buildcloudstorage.com/2012/07/significance-of-hadoop-running-on.html > Acesso em: 20 maio 2015.

CANALTECH CORPORATE (2013). **BYOD: A mobilidade e a insegurança de redes de mãos dadas**. Disponível em: http://corporate.canaltech.com.br/noticia/seguranca/BYOD-A-Mobilidade-e-a-Inseguranca-de-Redes-de-Maos-Dadas/ > Acesso em: 05 nov. 2014.

CANALTECH CORPORATE (2013). **Dicas de segurança corporativa para dispositivos móveis**. Disponível em: http://corporate.canaltech.com.br/dica/seguranca/Dicas-de-seguranca-corporativa-para-dispositivos-moveis/ > Acesso em: 05 nov. 2014.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e**

de informações. São Paulo. SENAC, 2006.

CHANNELPRONETWORK (2014). ***AirWatch enhances secure content locker with outlook plugin and social feed***. Disponível em: http://www.channelpronetwork.com/news/airwatch-enhances-secure-content-locker-outlook-plugin-and-social-feed > Acesso em: 12 dez. 2014.

CIO NBUSINESS (2015). **BYOD será prática corrente no Brasil a partir de 2014, revela estudo da Navita**. Disponível em: http://cio.com.br/noticias/2013/08/08/byod-sera-pratica-corrente-no-brasil-a-partir-de-2014-revela-estudo-da-navita/ > Acesso em: 29 de maio. 2015.

COBIT 5 FRAMEWORK PT, ISACA. São Paulo, 2012.

COMPUTER WEEKLY (2015). ***OpenStack Manila: File access storage for the open source cloud***. Disponível em: http://www.computerweekly.com/feature/OpenStack-Manila-File-access-storage-for-the-open-source-cloud > Acesso em: 21 maio 2015.

COMSTOR (2015). **7 dicas para obter sucesso em BYOD**. Disponível em: http://cdn2.hubspot.net/hub/240973/file-51175426-pdf/Comstor_Guia_7dicas_BYOD.pdf > Acesso em: 28 maio. 2015.

COMUNIDADE PORTUGUESA DE SEGURANÇA DA INFORMAÇÃO (2007). **Organizações certificadas**. Disponível em: http://ismspt.blogspot.pt/2005/11/organizaes-certificadas-quase-atingir.html > Acesso em: 10 out. 2014.

EYEOS S.L. (2012). **Site oficial da *EyeOS***. Disponível em: http://www.eyeos.com/ > Acesso em: 15 maio 2015.

GAEA CONSULTING (2005). **Compreendendo os principais conceitos do COBIT 5**. Disponível em: http://www.gaea.com.br/cms/compreendendo-os-principais-conceitos-do-cobit-5-parte-i/ > Acesso em: 05 jan. 2015.

GESTÃO EM TECNOLOGIA (2012). **Gestão de TI**. Disponível em: https://gestaoemtecnologia.wordpress.com/ > Acesso em: 21 nov. 2014.

ISO27K (2015). ***Information Security Standards***. Disponível em: http://www.iso27001security.com/index.html > Acesso em 15 jan. 2015

IT GOVERNANCE ONLINE (2015). ***ISO 27000 Series***. Disponível em: http://www.itgovernanceonline.com/information-security/iso-27000-series/ > Acesso em: 12 nov. 2014.

ITPORTAL, FEZ SISTEMAS (2013). **Mobilidade: Dispositivos Móveis e Segurança Corporativa**. Disponível em: http://home.fez.com.br/mobilidade-dispositivos-moveis-e-seguranca-corporativa/ > Acesso em: 20 out. 2014.

KASEYA BLOG (2013). ***Secure BYOD is about containing not restraining***. Disponível em: http://blog.kaseya.com/blog/2013/08/05/secure-byod-is-about-containing-not-restraining/> Acesso em 05 jan. 2015.

LAUREANO, Marcos; **Gestão de Segurança da Informação**, 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf > Acesso em: 21 nov. 2014.

LEVERAGE (2014). ***Kiteworks*, trabalhe de qualquer lugar**. Disponível em: http://www.leverage.inf.br/kiteworks.htm > Acesso em 17 jun. 2014.

MANAGIT. (2007). **Novidades do ITIL v3.** Disponível em: < http://managit.wordpress.com/2007/02/25/itil-v3-novidades/ > Acesso em: 10 set. 2014.

MANILA OPENSTACK PROJECT (2015). ***Welcome to Manila's developer documentation!*** Disponível em: http://docs.openstack.org/developer/manila/ > Acesso em: 21 maio 2015.

MANSUR, Ricardo. **Governança avançada de TI: na prática.** Rio de Janeiro. Brasport, 2009.

NEUPART INFORMATION SECURITY MANGEMENT (2002). **ISO 27001**. Disponível em: http://www.neupart.com/resources/iso-27001.aspx > Acesso 25 nov. 2014

OPENSTACK FOUNDATION (2015). **Site oficial da organização *OpenStack*.** Disponível em: https://www.openstack.org/ > Acesso em: 14 maio 2015.

PROFISSIONAIS DE TI – PTI (2013). **Política de Segurança para Aplicação BYOD**. Disponível em: http://www.profissionaisti.com.br/2013/06/politica-de-seguranca-para-aplicacao-byod/ > Acesso em: 11 jan. 2015.

PWC (2013). **Por que conhecer o COBIT 5?** Disponível em: http://www.pwc.com.br/pt_BR/br/10minutes/assets/10_min_cobits_14.pdf > Acesso em 11 jan. 2015.

RISK IT, ISACA (2009). ***The Risk IT Framework - Excerpt***. Disponível em: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-

Framework-Excerpt_fmk_Eng_0109.pdf > Acesso em 07 jan. 2015.

THINGS THAT RESONATE (2012). ***Gartner ITxpo Gold Coast***. Disponível em: https://thingsthatresonate.wordpress.com/2012/11/16/gartner-itxpo-gold-coast/#more-471 > Acesso em: 07 jan. 2015.

UNIVERSIDADE VEIGA DE ALMEIDA (2015). **Política de Segurança da Informação – ANEXO I – BYOD**. Disponível em: http://www.uva.br/pdfs/politica-seguranca-informacao-anexo-byod.pdf > Acesso em: 10 jan. 2015.

VAL IT, ISACA (2006). ***Enterprise Value: Governance of IT Investments - The Business Case***. Disponível em: http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Documents/VAL-IT-business-case.pdf > Acesso em: 08 jan. 2015.

VIVA O LINUX (2015). Novo EyeOS – Sistema Operacional de Computação nas Nuvens. Disponível em: http://www.vivaolinux.com.br/artigo/Novo-EyeOS-Sistema-Operacional-de-Computacao-nas-Nuvens?pagina=1 > Acesso em: 07 maio 2015.

VMWARE | BLOGS (2015). ***A closer look at AirWatch***. Disponível em: http://blogs.vmware.com/cto/closer-look-airwatch/ > Acesso em: 10 dez. 2014.

VMWARE BRASIL (2015). ***VMware + Openstack.*** Disponível em: http://vmwarebrasil.blogspot.com.br/2014/11/vmware-openstack.html > Acesso em 16 maio 2015.

VMWARE NEWS RELEASES (2014). **Aquisição da *AirWatch* pela *VMware***. Disponível em: https://www.vmware.com/br/company/news/releases/airwatch-port-012214 > Acesso em: 15 dez. 2014.

WALTON, Richard E. **Tecnologia de Informação: O uso de TI pelas empresas que obtêm vantagem competitiva.** São Paulo. Atlas, 1998.

WEBINSIDER (2008). **ITIL e a segurança da informação**. Disponível em: http://webinsider.com.br/2014/04/21/itil-e-a-seguranca-da-informacao-parte-i/ > Acesso em: 07 dez. 2014