Universidade do Minho
Escola de Economia e Gestão

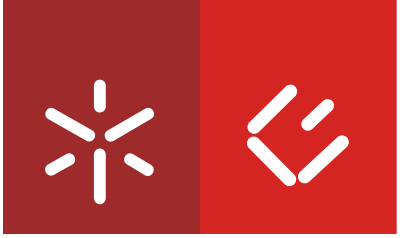
Fortunato António André

Gestão da Segurança da Informação: Importância da Sua Adopção em Pequenas e Médias Empresas Angolanas

dezembro de 2014

Fortunato António André **Gestão da Segurança da Informação: Importância da Sua Adopção em Pequenas e Médias Empresas Angolanas**

UMinho | 2014



Universidade do Minho
Escola de Economia e Gestão

Fortunato António André

Gestão da Segurança da Informação: Importância da Sua Adopção em Pequenas e Médias Empresas Angolanas

Dissertação de Mestrado
Mestrado em Estudos de Gestão

Trabalho efetuado sob orientação do
Professor Doutor José António Crispim

dezembro de 2014

DECLARAÇÃO

Nome: Fortunato António André

Endereço Electrónico: fortunatoao@yahoo.com.br Telefone: 244 924 792789

Número do Bilhete de Identidade: 002553252LA039

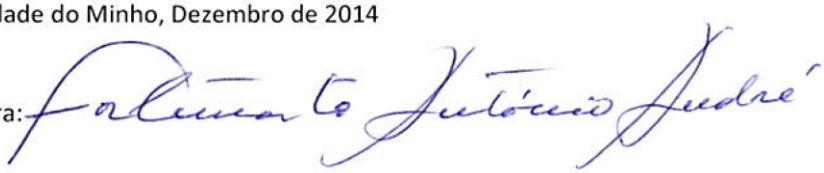
Título dissertação: Gestão da Segurança da Informação: Importância da Sua Adopção em Pequenas e Médias Empresas Angolanas.

Orientador: Professor Doutor José Almeida Crispim. Ano de conclusão: 2014

Designação do Mestrado: Estudos de Gestão.

AUTORIZO A REPRODUÇÃO INTEGRAL DESTA TESE, MEDIANTE DECLARAÇÃO ESCRITA DO INTERESSADO, QUE A TAL SE COMPROMETE.

Universidade do Minho, Dezembro de 2014

Assinatura: 

Aos meus filhos:

Elisângela André
Érica André
Tiago André
Hugo André

AGRADECIMENTOS

À Deus pela força e iluminação à minha vida. Aos meus pais pela educação, paciência e dedicação para tornar-me no que sou hoje. A minha família, esposa e filhos pela compreensão da falta de atenção em alguns momentos.

Ao meu orientador Doutor José António Almeida Crispim, pela orientação e confiança depositada na realização deste trabalho.

À todos que participaram nas entrevistas para a realização da pesquisa. Aos meus colegas do PAG "programa avançado de gestão".

Aos meus amigos pelo incentivo e á todos os professores do PAG pelo conhecimento transmitido.

RESUMO

A crescente dependência das Tecnologias de Informação (TI) nas empresas tem despertado aos seus gestores uma mudança de abordagem quanto a visão da segurança da informação que em muitos casos ainda está voltada para o aspeto tecnológico. Embora grande parte das informações cruciais para o negócio estejam guardados em computadores, também é necessário, considerar a proteção das informações em papel, transcritas pelos órgãos de decisão da empresa. A dependência às TI acarreta riscos que colocam em perigo as informações confidenciais, íntegras e disponíveis das organizações. Esta dependência faz da Gestão da Segurança da Informação (GSI) um importante instrumento na gestão de negócio. Assim, as empresas devem necessariamente compreender que a segurança da informação é, hoje, um problema de negócio e não apenas de tecnologia. O tema em estudo mostra-se relevante pelo fato da informação ser um recurso indispensável para o negócio de qualquer tipo de empresa e necessitar ser adequadamente protegida de modo a assegurar a sua confidencialidade, integridade e disponibilidade (CID). O trabalho consistiu num caso de estudo que envolveu três organizações angolanas, instaladas em Luanda, com o intuito de mostrar as razões das pequenas e médias empresas em adotarem a gestão da segurança da informação, verificar em que medidas as realizam e analisar se as práticas de segurança da informação adotadas podem garantir a continuidade de seu negócio em caso de incidente. Foram feitas entrevistas semi-estruturadas com os seus gestores de TI, que foram analisadas e comparadas. Os dados mostram que as medidas de protecção da informação mais utilizada é o antivírus e o *firewall* e foram unânimes de que o receio de perda financeira é um dos pontos que as levam a adoptarem a gestão da segurança da informação.

Palavras-chave: Segurança da Informação; Gestão da Segurança da Informação; Políticas de segurança; Gestão de riscos e pequenas e médias empresas.

ABSTRACT

The growing number of information technology (IT) in the business environment, coupled with the increasing reliance of information systems in organizations, makes the management of Information Security an important tool in corporate management. The aim of this study is to investigate to which extent small and medium sized enterprises (SME), perform security management information and identify the reasons that lead them to adopt management measures for information security. The importance of the topic under study, is due to the fact that the information is a necessary resource for the success of virtually any type of business today and needs to be properly protected to ensure the confidentiality, integrity, availability of the information. This work consists of a case study in three Angolan organizations, installed in Luanda, in order to identify the reasons why small and medium sized enterprises adopt the management of Information Security. Furthermore, it verifies the performance of the measures and analyzes whether the security practices of information taken can ensure the continuity of a business in case of an incident. The interviews were semi-structured with the corporate TI managers, which were analyzed and compared. The data shows that the most widely used measures to protect information is Antivirus-protection and were unanimous that the fear of financial loss is one of the points that lead the enterprises to adopt the management of Information Security.

Key-words: Information Security; Information Security Management; Security Policies; Risk Management and small and medium enterprises.

Índice

LISTA DE SIGLAS

ANIP	Agência Nacional de Investimento Privado
CID	Confidencialidade, Integridade e Disponibilidade
DTI	Direção de Tecnologia da Informação
GR	Gestão de Risco da Segurança da Informação
GSI	Gestão da Segurança da Informação
IEC	International Electrotechnical Commission
INAPEM	Instituto de Apoio as Pequenas e Médias Empresas
ISMS	Information Security Management System
ISO	International Organization Standardization
MPME	Micro, Pquenas e Médias Empresas
PC	Personal Computer
PCN	Plano de Continuidade de Negócio
PDCA	Plan, Do, Check, Act
PSI	Política de Segurança da Informação
SI	Segurança da Informação
SGSI	Sistema de Gestão da Segurança da Informação
TI	Tecnologia da Informação

LISTA DE FIGURAS

LISTA DE TABELAS

CAPÍTULO I - INTRODUÇÃO

Angola, oficialmente República de Angola, é um país da costa ocidental de África, cujo território principal é limitado a norte e a nordeste pela República Democrática do Congo, a leste pela Zâmbia, a sul pela Namíbia e a oeste pelo Oceano Atlântico. Inclui também o enclave de Cabinda, através do qual faz fronteira com a República do Congo, a norte. Para além dos países vizinhos já mencionados, Angola é o país mais próximo da colónia britânica de Santa Helena (território).

A República de Angola é hoje, um país emergente, com novas oportunidades em termos de crescimento e desenvolvimento socioeconómico, graças a estabilidade política alcançada há 12 anos, após longo período de guerra desde a conquista da independência em 1975 até ao seu termo, em Abril de 2002.

A estabilidade política tornou o mercado, mais abrangente, marcado na diversidade de negócios, fruto do aumento de empresas que operam no mercado nacional, como empresas locais e estrangeiras que contribuem para o crescimento económico e melhoria da situação de vida da população, alvo de carências, devido ao longo período de guerra que devastou o país.

O aumento, cada vez maior, de empresas dos mais variados setores da economia angolana é um indicador da dependência crescente do negócio à tecnologia de informação. Pois, a TI como provedora de serviço, participa cada vez mais nos negócios das empresas. O seu uso simplifica o trabalho nas organizações, mas também expõe as suas informações ou ativos da informação à ameaças que consequentemente despertam a necessidade de se prover recursos para o seu controlo.

Um banco inevitavelmente recorre ao suporte tecnológico para a execução da sua atividade, que vai desde a abertura da conta, processos de transferência, depósito e levantamento de valores entre outras operações. O risco de sofrer um ataque é elevado tendo em conta a natureza do seu negócio.

Como grande parte das transações são efetuadas através de computadores e por armazenar elevado número de informações críticas, é necessário que sejam tomadas medidas adequadas para mitigar os riscos eminentes de modo a que se torne inviolável a confidencialidade, a integridade e a disponibilidade das informações.

1.1 QUESTÃO PROBLEMA

Atendendo a importância de se elevar os níveis de cultura com relação a segurança da informação nos círculos das pequenas e médias empresas angolanas, este estudo visou verificar porquê da adoção da gestão da segurança da informação em PMEs, em particular as organizações do sector bancário. O estudo centrou-se fundamentalmente em dois pontos de interesse que são:

- Política de segurança da informação; e
- Gestão de riscos de segurança da informação.

Para o efeito foram observados os procedimentos constantes das normas ISO 27001 e 27002. Neste contexto surgiram as seguintes questões:

- Como as organizações estudadas realizam gestão da segurança da informação?

- Quais as actividades e procedimentos adotados para a gestão da segurança da informação podem garantir a continuidade do negócio?

- Como as boas práticas de gestão da segurança da informação podem garantir a continuidade do negócio?

1.2 OBJECTIVOS

1.2.1 Objectivo Geral

Este trabalho visa investigar por que é importante as pequenas e médias empresas angolanas adotarem a gestão da segurança da informação como ferramenta indispensável na sua estratégia de negócio. Será utilizado um estudo de caso que envolverá três bancos de pequeno e médio porte, centrando-se especificamente em duas abordagens como a política de segurança da informação e a gestão de risco de segurança da informação.

1.2.2 Objectivo Específico

- Verificar como as pequenas e médias empresas realizam a gestão da segurança da informação;
- Identificar e relatar as atividades e procedimentos adotados para a gestão da segurança da informação;

- Demonstrar como as boas práticas de gestão da segurança da informação são um meio necessário para garantir a continuidade do negócio em caso de ocorrência de um incidente;

1.3 JUSTIFICAÇÃO DA IMPORTÂNCIA DO TEMA

A gestão da segurança da informação é hoje, vista, pelas organizações, como uma ferramenta de valor na gestão de negócio. Sendo cada vez mais indispensável os recursos de tecnologia de informação (TI), mais dependentes e expostos à riscos, encontram-se as organizações que, por esta razão procuram formas de proteger o seu negócio.

Grande parte dos gestores de empresas, à nível global, tem mostrado interesse em ver o seu negócio protegido dos riscos inerentes. Assim, aclamam pela gestão da segurança da informação, que é vista, como um veículo a que se pode guiar para a protecção do negócio, independentemente do mercado em que está envolvido, pois as informações são necessárias para a gestão de qualquer tipo de negócio e, se perdem-nas, abre-se um fosso. Mas, na verdade, existem ainda empresas que ignoram as práticas de gestão da segurança da informação (GSI) por não a considerarem como um elemento essencial na sua estratégia de negócio. Consideram apenas os recursos tecnológicos como único meio para a segurança da informação. Deste modo, urge em Angola, a necessidade de se promover cultura de gestão da segurança da informação para o conhecimento e consciencialização de que a Segurança da Informação não se esgota apenas nos recursos tecnológicos, pois é mais abrangente.

Notamos, hoje, que o mundo dos negócios é cada vez mais competitivo. E para manter a sobrevivência competitiva é fundamental as organizações sensibilizarem-se da importância que tem a SI, baseada nas melhores práticas de gestão e perceberem que a GSI também está para os pequenos e médios negócios e não somente para as grandes instituições. Neste contexto e com o crescimento da economia angolana, vista, como uma das que mais cresce no mundo, tem surgido vários bancos e atendendo a natureza de seu negócio, uma vez que trabalham com informações dos clientes e sendo estas sensíveis, devem estar sensibilizados da necessidade de proteção de seus ativos de informação.

Pretende-se, com este estudo, investigar por que atualmente a SI deve ser parte integrante da gestão de negócio das PME´s, com particular destaque as empresas angolanas. O tema, também pode fornecer dados importantes que sirvam para um melhor entendimento sobre a

gestão da segurança da informação, assim como os benefícios que pode trazer às empresas com a sua implementação. A política de segurança da informação e a gestão de risco de segurança da informação são elementos indispensáveis na gestão de segurança da informação por dotar a empresa de regras e métodos eficazes para o controlo de riscos inerentes.

1.4 Delimitação do Estudo

Esta pesquisa está confinada às Pequenas e Médias empresas angolanas do setor bancário, localizadas em Luanda - Capital de Angola, pelo que constituem o foco deste trabalho.

1.4 ESTRUTURA DO TRABALHO

O presente estudo, está organizado em capítulos, a saber:

- No capítulo 1 é apresentada a introdução deste trabalho;
- No capítulo 2 é apresentado o conceito de segurança da informação e outros aspetos importantes relacionados com a gestão da segurança da informação;
- O capítulo 3 aborda sobre a metodologia aplicada a pesquisa do estudo;
- O capítulo 4 apresenta o estudo de caso realizado em três organizações;
- O capítulo 5 trata da análise e discussão dos resultados;
- O capítulo 6 apresenta a conclusão do trabalho.

CAPÍTULO II - REVISÃO DA LITERATURA

2.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é essencial para a proteção das informações cruciais de uma organização, sujeitos a ameaças que podem colocar em risco o seu negócio. Por esta razão, a SI revela ser uma das principais prioridades na gestão de negócio de uma empresa. Mas, convém antes, de se discorrer sobre a questão segurança da informação, fazer uma breve abordagem sobre a informação em si para melhor se entender a importância que tem para o negócio e por que necessita ser protegida.

A informação é um ativo que, como outros ativos importantes para o negócio, é fundamental para uma organização e necessita ser protegida de forma adequada. É importante para os negócios, a proteção da informação, devido ao aumento cada vez maior da conexão entre ambientes de trabalho. Pois, com este aumento, a informação fica mais exposta a uma variedade de ameaças (BS ISO/IEC 27002, 2005).

A informação, é hoje, considerada o bem mais valioso de uma empresa. Pois, Conforme Caruso e Steffen (1999, p. 21), *"(..) o bem mais valioso de uma empresa pode não ser o produzido pela sua linha de produção ou o serviço prestado, mas as informações relacionadas com esse bem de consumo ou serviço"*. Os mesmos autores afirmam que as informações são de valor inestimável tanto para a empresa (dona da informação), como também para a concorrência e, neste contexto devem ser protegidas. Sêmola (2003), corrobora afirmando que a informação é um ativo cada vez mais valorizado e, indispensável na gestão de negócio, porque as organizações elaboram o seu plano de negócio baseando-se em informações. E assim procuram preservá-las dos riscos que advêm das ameaças por explorarem vulnerabilidades.

Segundo Caruso & Steffen (1999, p. 22):

> *"Da mesma forma que seus ativos tangíveis, as informações envolvem os três factores de produção tradicionais: capital, mão-de-obra e os processos. Assim, ainda que as informações não sejam passíveis do mesmo tratamento fisco-contábil que os outros ativos, do ponto de vista do negócio elas são um ativo da empresa e, portanto, devem ser protegidas."*

A informação é de fato, o principal elemento para o sucesso do negócio de uma organização, daí a necessidade premente de ser protegida, de modo a manter a empresa, capaz das suas necessidades, elevando-se os níveis de competitividade.

Pois, conforme diz Raggad (2010) a capacidade de uma empresa gerar negócios e ser bem sucedida é impulsionada pela informação. Se a informação for precisa, completa e oportuna, então, haverá sucesso no negócio, caso contrário, a geração de valor ao negócio será fraca. Esta informação também é a base da vantagem competitiva. Se um rival se apodera de algumas dessas informações, as consequências poderão ser desastrosas, assim como um concorrente que consiga interceptar a troca de informações relacionadas com custos e preços entre dois parceiros, pode causar perdas avultadas ao negócio.

A informação precisa ser protegida, independentemente da forma como se apresenta. A segurança da informação é o recurso apropriado para a proteção da informação, pois ela cobre todos os aspetos que a informação pode tomar.

A segurança da informação inclui todos os aspectos da informação, seja falada, escrita, impressa, eletrónica, ou relegada a qualquer outro meio de comunicação, independentemente de estar a ser criada, modificada, analisada, transportada, armazenada, ou destruída (Brotby, 2009).

O objetivo da segurança da informação é a preservação da CID (confidencialidade, integridade e disponibilidade).

Assim, para a BS ISO/IEC 27002 (2005), segurança da informação é um recurso essencial para a protecção da informação contra os vários tipos de ameaças a fim de garantir a continuidade do negócio, a minimização dos riscos e maximização do retorno sobre os investimentos e oportunidades de negócios. O seu resultado permite a organização manter vantagem competitiva, o fluxo de caixa, a rentabilidade e particularmente a imagem comercial.

Com a atual dependência do negócio à tecnologia de informação, as organizações procuram proteger as suas informações estratégicas armazenadas nestes ambientes para impedir a quebra de um ou mais princípios de segurança, de modo a manter a estabilidade funcional da empresa e, garantir assim, o seu sucesso. Neste sentido, Sêmola (2003) afirma que toda informação numa organização é influenciada por três princípios básicos que são a

confidencialidade, integridade e disponibilidade. Para o autor, a segurança da informação é a preservação desses elementos, além de outros aspetos que podem estar envolvidos como a autenticidade e a legalidade.

A TI pode proporcionar a uma empresa, maior rapidez na execução das suas ações de negócio, ajudando a administração na tomada de decisão através de informações relevantes, mas, ao mesmo tempo, fragiliza as informações, expondo-as a riscos, que se não forem tomadas medidas de segurança para o seu controlo, podem causar danos avultados no negócio. Neste contexto, a SI não deve ser descurada, pois para Beal (2005), a segurança da informação é o processo de proteger as informações de qualquer tipo de ameaças, com vista a manter inviolável a confidencialidade, integridade e disponibilidade.

Segundo Gelbstein e Kamal (2002), a definição formal de segurança da informação baseia-se em dois critérios:

- Ativos, ameaças, vulnerabilidades e risco residual;
- Confidencialidade, integridade e disponibilidade.

De acordo com as ideias destes autores, podemos definir a segurança da informação como sendo a protecção da informação contra os diversos tipos de ameaças à confidencialidade, integridade e disponibilidade, de modo a garantir a continuidade do negócio e reduzir os riscos.

A maioria das empresas, em todo mundo, concorda que os objetivos de segurança adotados são aqueles que constituem a tríade CID (confidencialidade, integridade e disponibilidade).

De acordo com Wheeler (2011), os três pilares básicos de segurança da informação são:

- Confidencialidade
- Integridade
- Disponibilidade

Segundo o autor, a **confidencialidade** é a garantia de que a informação não é divulgada a pessoas ou entidades estranhas, pois o acesso à informação da empresa é somente para aqueles que estejam devidamente autorizados.

A **Integridade** consiste em garantir que a informação permaneça exata, sem sofrer modificação ou destruição, que possa comprometer a sua autenticidade.

A **Disponibilidade** é a garantia de que a informação esteja disponível para o acesso confiável e sempre que necessário a todos os utilizadores autorizados.

John McCumber (2005), assevera que a principal consideração para a confidencialidade não é simplesmente manter o segredo da informação, mas sim, torná-la disponível apenas para aqueles que precisam, quando precisam, e sob circunstâncias apropriadas. A integridade sendo crítica, deve garantir que informações precisas estejam sempre disponíveis. Por outras palavras, a integridade proporciona precisão e robustez dos dados. Finalmente, a disponibilidade na visão do autor representa a atualidade dos dados. Se os dados estiverem inacessíveis quando necessário, então a informação não está disponível.

O autor Raggad (2010), é de opinião que as três metas de segurança (confidencialidade, integridade e disponibilidade), não são suficientes para os objetivos de segurança, pois na sua visão, outras características de segurança devem ser adicionadas, como a autenticidade e o não-repúdio.

A Figura 1 mostra as metas de SI, segundo Raggad (2010).

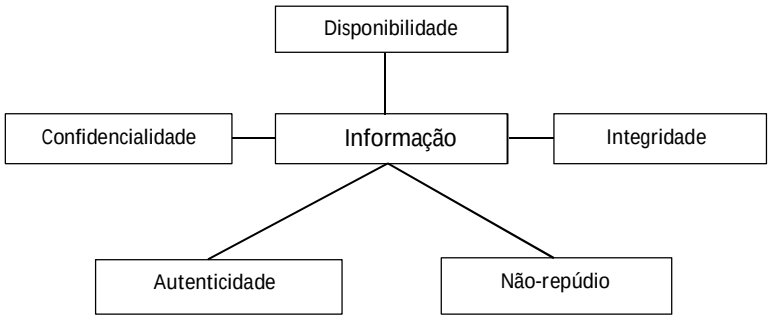


Figura 1 – Princípios de Segurança da Informação
Fonte: Adaptado de Raggad (2010)

A **autenticidade**, visa garantir que a fonte de uma determinada mensagem é legítima, assim como a autoria da informação enviada é válida, isto é, a informação após o seu envio ou validação deve ser precisamente aquela que o remetente enviou sem alteração, dando garantia de integridade ou de segurança da informação.

O **não-repúdio**, implica que duas entidades num processo de comunicação não podem negar o seu envolvimento nesse processo, isto é, o remetente não pode negar o envio da informação, assim como o destinatário não pode negar ter recebido. A assinatura digital é um meio de impôr não-repúdio no uso da internet ou *e-mail*, pois são mantidas, diariamente, comunicações internas e externas através destes meios, sendo dessa forma, necessário saber a origem das mensagens para certificar se o remetente é quem realmente diz ser.

Uma organização, para manter os seus ativos de informação assegurados contra eventuais riscos, deve adotar um conjunto de controlos de segurança. Esses controlos, devem ser revistos e aperfeiçoados de tempo à tempo para permitir a organização mantê-los atualizados contra os riscos e assim garantir que os objetivos do negócio e de segurança sejam alcançados. Para o caso, a gestão do risco é importante, por ser uma ferramenta poderosa na gestão da segurança da informação, e envolver processos como a análise/avaliação do risco e o tratamento do risco que provêem, uma visão, sobre o que necessariamente, deve ser protegido das ameaças a que está sujeito, para depois, serem apresentadas medidas de proteção adequadas para a mitigação ou diminuição dos riscos do negócio.

2.2 GESTÃO DO RISCO DE SEGURANÇA DA INFORMAÇÃO

A adoção de uma abordagem de gestão, sustentada nos riscos inerentes ao negócio é de suma importância para o alcance dos objetivos de segurança de uma empresa, pois conhecer as ameaças e as vulnerabilidades a que estão sujeitas, assim como o impacto que ocorreria se a segurança fosse quebrada, ajuda na tomada de decisão sobre como e quanto gastar com a segurança para manter os ativos da informação protegidos de ameaças à confidencialidade, integridade e disponibilidade (Beal, 2005).

Caruso e Steffen (1999, p. 35) alertam como segue:

> *"Cada vez mais as organizações humanas tornam-se dependentes de informações armazenadas em computadores. Aproveitam-se a grande velocidade e a capacidade de cruzamento de informações que os computadores possuem para se obterem beneficios como rápida tomada de decisões, mudança rápida de estratégia e/ou tática, etc. Mas a mesma facilidade proporcionada pelos computadores também implica alto risco de violação. O mesmo programa usado para emitir um relatório de projeção de vendas, destinado ao diretor de marketing, pode ser usado por um "espião" para emiti-lo para o diretor de marketing do concorrente."*

A gestão de risco de segurança da informação traz benefícios para a organização. É importante para o controlo eficaz dos riscos.

Segundo Dantas (2011, p. 71):

> *Um dos principais benefícios da gestão de risco é poder garantir o desenvolvimento das atividades de negócio dentro de um ambiente de controle permanente sobre os riscos, pois, (…) o ambiente de negócios é altamente mutável e repleto de incertezas. E a capacidade de convivência nesse cenário, mediante um processo austero de gestão, é um fator decisivo de vantagem competitiva e de sucesso nos negócios.*

Neste contexto, e de acordo com Humphreys (2010), todas as organizações devem estar cientes da necessidade de se gerir os riscos de segurança da informação[1].

Risco é a probabilidade de um evento não desejado acontecer, como o vazamento de informações, destruição da informação ou negação de serviço, que daria lugar a consequências graves no negócio, como prejuízo financeiro. O risco, está geralmente, ligado às oportunidades de agentes (ameaças) explorarem vulnerabilidades dos ativos de informação (Raggad, 2010).

Para Beal (2005, p. 11) a gestão de riscos é definida como sendo:

"(...) o conjunto de processos que permite às organizações identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos".

A gestão de risco na visão de Raggad (2010), é um processo sequencial que visa identificar os riscos a que os recursos de informação utilizados por uma organização estão expostos, de modo a serem tomadas medidas necessárias para reduzir o risco à um nível aceitável de acordo o valor que o recurso de informação tem para a organização. Este processo inicia-se com a identificação do risco, a avaliação do risco que estuda os efeitos das ameaças sobre os ativos e, por fim, a mitigação dos riscos, feita através de controlos de segurança apropriados.

A gestão do risco, sendo um processo relevante no contexto da gestão da segurança da informação e conforme mostrado na Figura 4, consiste segundo Raggad (2010), de um conjunto de fases sequenciais e documentadas.

[1] Portanto, qualquer organização independentemente do seu porte ou tamanho, que tem como suporte das suas atividades a TI deve pautar por organizar um processo de controlo de risco, a fim de manter seguro o negócio.

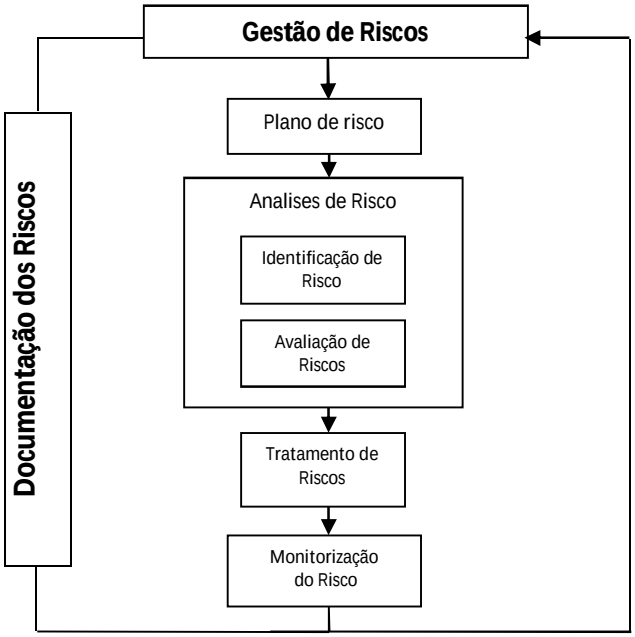


Figura 2 - Fases da gestão do risco de segurança da informação
Fonte: Raggad (2010)

Como podemos aferir, a GR inclui no seu processo, atividades como: plano de risco, análise de risco, avaliação de risco, tratamento de risco e monitorização do risco.

O **Plano de Risco** é o documento que engloba uma estratégia abrangente e interativo com métodos de identificação e rastreamento de riscos, avaliações contínuas de riscos, planos de tratamento de riscos para determinar como modificar os riscos e fornecer recursos adequados de proteção.

A **Análise de risco**, descreve a origem do risco, examina o risco identificado de modo a reduzir os seus efeitos. Ela inclui a identificação de risco e avaliação de risco que define os incidentes de risco de acordo à sua probabilidade de ocorrência e gravidade do impacto ou consequências.

Após, a identificação dos riscos, a **Avaliação do risco** visa determinar o nível do risco identificado e medir a probabilidade e o impacto potencial da ocorrência. Ela (avaliação do risco) é necessária, pois antes de qualquer tratamento de risco ser aprovado pela direção da empresa, os riscos avaliados são comparados com os benefícios esperados.

O **Tratamento de risco** é o processo de seleção e implementação de controlos de segurança, a fim de reduzir os riscos à nivéis aceitáveis.

A **Monitorização do risco** é o processo que avalia e acompanha sistematicamente a performance das ações de tratamento de riscos e de acordo com a necessidade, desenvolve novas opções de tratamento de risco. Este processo verifica as diferentes atividades de gestão de riscos.

Quanto a **Documentação do risco**, ela descreve as várias fases da gestão do risco.

A gestão do risco para a autora Beal (2005, p. 17):

" (…) precisa contemplar várias etapas cíclicas que levam à redução do risco, indo da análise ao tratamento, aceitação e comunicação". A aceitação do risco, segundo a autora, é a decisão de aceitar um risco.[2]*"*

Wheeler (2011), alerta que os riscos aceitáveis não devem limitar o crescimento da empresa, pois uma empresa pode aumentar as suas oportunidades de negócios se pensar em segurança da informação como forma de manter os riscos a que está exposta dentro dos níveis aceitáveis. A organização ao iniciar um negócio de risco que pode proporcionar vantagem competitiva, tem que reduzir os riscos e transferi-los para outras áreas para poder ter um espaço de tolerância ao risco. Isto permite a organização assumir riscos de negócios que daria vantagens sobre seus concorrentes.

A comunicação do risco, refere a informação que é transmitida acerca dos riscos identificados e que tenham sido tratados, aceites ou não. Todas as partes envolvidas no processo, recebem esta informação.

Na visão de Wheeler (2011), após o processo de avaliação do risco é importante medir e priorizar os riscos para a tomada de decisão sobre que riscos precisam ser abordados e até que ponto é apropriado mitigá-los. Para o autor, o foco da mitigação de riscos não é eliminar completamente o risco, mas sim reduzí-lo a um nível aceitável. Isto significa que a empresa para mitigar ou tornar menos intenso o risco precisa:

- Reduzir a probabilidade de ocorrência;
- Limitar a gravidade do impacto ou;
- Reduzir a sensibilidade do recurso.

[2] A aceitação de um risco pode acontecer quando o custo de proteção é maior que o custo do próprio ativo que se pretende proteger. Pode também ocorrer quando os riscos identificados, encontram-se já nos níveis aceitáveis.

A Figura abaixo mostra como é gerado um risco, o que pode provocar quando ocorre e como proteger-se dele.

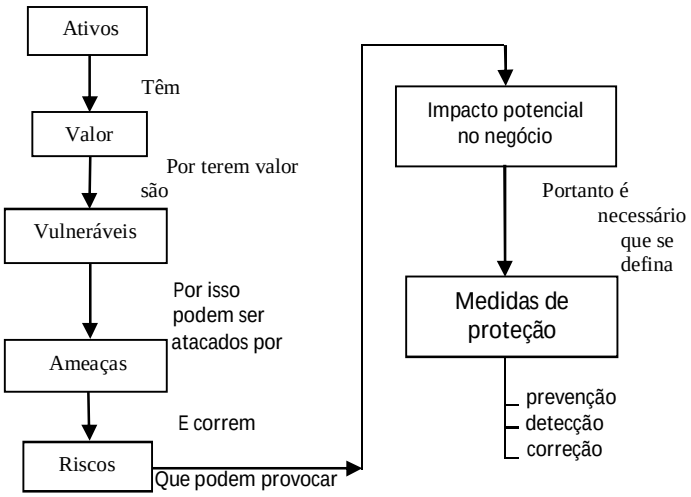


Figura 3 – Avaliação de Risco e Medidas de protecção.
Fonte: Elaboração com base na ISO/IEC 27001.

Fazendo menção a Figura 5, notamos que os ativos por terem valor são vulneráveis. As vulnerabilidades sendo fraquezas associadas aos ativos podem ser exploradas por ameaças que geram riscos que podem provocar impacto no negócio. Daí a necessidade de medidas de proteção adequadas para o controlo dos riscos.

A seguir, está apresentado um descritivo dos termos ativo, vulnerabilidade e ameaça, por serem partes indispensáveis da segurança da informação.

2.2.1 Ativo

Um ativo é qualquer coisa que uma organização atribui valor. São especificamente relevantes para a segurança da informação os seguintes elementos que se enquadram na categoria de ativos: documentos, base de dados, *software*, bens físicos de TI (computadores, redes, etc.), reputação e imagem (Gelbstein e Kamal, 2002).

Para Sêmola (2003) e Beal (2005), ativo é toda informação que tem valor para o negócio, assim como os recursos que fazem parte do processo de manuseamento da informação, incluindo informações cruciais, detida pelas entidades que têm poder de decisão na organização, bem como os recursos de *hardware* e *software*.

Mas, atenção que, de acordo com a ISO/IEC 27001:2005 os ativos não incluiem necessariamente, tudo que normalmente uma organização considera que tem valor[3]. Portanto, o valor de um ativo pode ser determinado através do impacto que tem no negócio quando ocorre um incidente. Pode acontecer um incidente quando um ativo apresenta vulnerabilidade que pode ser explorada por uma ameaça.

2.2.2 Vulnerabilidade

Vulnerabilidade é o ponto fraco ou a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (BS ISO/IEC 27002:2005).

A autora Beal (2005) considera a vulnerabilidade como uma fraqueza que pode ser explorada por uma ameaça com objetivo de materializar um ataque. Já Sêmola (2003), assevera como sendo uma debilidade aliada aos ativos que são susceptíveis de serem exploradas por ameaças, que ao ocorrer pode gerar um incidente e, assim, afetar os princípios de segurança da informação. Deste modo, podemos afirmar que vulnerabilidade é a parte delicada de um ativo que é passível de ser explorada por uma ameaça, que ao suceder, pode causar prejuízos no negócio de uma organização.

> *Ameaças exploram vulnerabilidades para atingir alvos de ataque. As vulnerabilidades determinam o grau de exposição de um ativo de informação, ambiente ou sistema a determinada ameaça. A falta de treinamento dos usuários, por exemplo, representa uma vulnerabilidade em relação à ameaça de erro humano, assim como a instalação de um data center[4] (Beal, 2005, p. 18).*

Mas, salienta-se que, "*As vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou condição favorável, que são as ameaças*" (Sêmola, 2003, p. 48).

Para se compreender melhor sobre as vulnerabilidades, o Quadro 3 mostra exemplos de vulnerabilidades que podem existir numa determinada empresa.

[3] A organização deve decidir que ativos podem afetar a entrega de um produto ou serviço pela sua ausência ou deterioração, ou podem causar prejuízo à organização através de perda de disponibilidade, integridade ou confidencialidade.
[4] Centro de processamento de dados, local onde se encontram instalados os equipamentos (servidores), responsáveis pelo fornecimento dos serviços à atividade de uma empresa.

CONSULTORES	INSTALAÇÃO	BASE DE DADOS
. Contratação Inadequada . Falta de Consultores	. Falta de mecanismo de Monitorização . Proteção física inadequada . Energia elétrica instável	. Falta de cópias de segurança (backup) . Armazenamento de dados Inadequado

Tabela 1 – Exemplos de Vulnerabilidades
Fonte: Elaboração própria

Com base nos exemplos acima, denota-se que são vários os eventos de segurança que podem facilitar uma ameaça a realizar uma acção.

2.2.3 Ameaça

Ameaça é a fonte potencial de um incidente que pode provocar danos numa organização (BS ISO/IEC 27002, 2005).

Para Sêmola (2003), ameaça é um agente que ao explorar vulnerabilidades, coloca em risco as informações e seus ativos de informação e causa incidentes que podem acarretar impactos negativos à organização com a perda de confidencialidade, integridade e disponibilidade.

Uma ameaça pode acontecer de forma acidental ou deliberada, motivada por um agente que, pode afetar o ambiente de uma organização. A ameaça procura identificar a fragilidade (vulnerabilidade) de um ativo com vista a realizar um ataque que ao consumar-se dá origem a uma falha de segurança (Beal, 2005). Seguindo as ideias destes autores, podemos afirmar que ameaça é um evento que pode causar impacto de diferentes níveis no ambiente de negócio de uma empresa.

A informação é o elemento alvo de ataque de uma ameaça, que em caso de ocorrência, pode causar prejuízos enormes à uma organização. Desta forma e, considerando a existência de vários tipos de ameaças, é importante categorizá-las para conhecer-se os tipos de ameaças que são causadas de forma intencional e aqueles que são por efeitos da natureza. Assim, Raggad (2010, p. 82), classifica as ameaças da seguinte forma:

- Naturais;
- Acidentais e;
- Intencionais.

- **Ameaças naturais**, estão relacionadas com as condições do meio ambiente. São procedentes de fenómenos da natureza e ocorrem de forma aleatória.

- **Ameaças acidentais**, estão associadas ao erro humano, cometido por um indivíduo e erros nos processos, etc., causados de forma involuntária. Esse tipo de ameaça não é planeado.

- **Ameaças intencionais**, são ataques feitos pelo homem de forma deliberada. O ataque pode resultar em acesso não autorizado, divulgação ou alteração de dados confidenciais, negação de serviços, ou outros efeitos planeados pelos atacantes. As ameaças intencionais são geralmente motivadas pelo ganho de algum bem ou outras oportunidades, causando prejuízos as vítimas.

O Quadro abaixo, mostra exemplo de uma diversidade de ameaças, que podem colocar o negócio de uma organização em risco.

Tipo de Ameaças	Efeitos da Ameaça ao Ativo	Impacto e Consequências da Ameaça
Ameaças Naturais		
Terramotos, incêndios inundações, tempestades, falta de energia	Falta de energia, incêndios	A perda ou degradação das comunicações, destruição de equipamento.
incidentes biológicos	Doenças, morte de especialistas em segurança	Interrupção das funções / negação de serviço
Ameaças acidentais		
Erro do utilizador	Ficheiro / exclusão de dados, manuseio de equipamentos, entrada inválida	Interrupção das funções / modificação não autorizada de dados.
Erro do administrador	Erros de configuração de ativos de informação	Acesso não autorizado ao ativo de informação, o que pode levar à divulgação distinta do titular da informação, alteração de dados, interrupção dos serviços ativos e ações enganosas.
Hardware / falha de software	Falha de servidores, a perda de ligação à Internet, a falha dos dispositivos de comunicação.	Interrupção das funções / serviços, a destruição de equipamentos, a modificação não autorizada de dados.
Ameaças intencionais		
Hackers	Quebra de senhas, espionagem, falsificação, cavalos de Tróia, vírus.	A divulgação não autorizada de informações e acesso não autorizado ao ativo de informação, o que pode levar à divulgação não autorizada de informações, alteração de dados, interrupção dos serviços ativos e ações enganosas.

Tabela 2 - Exemplos de Ameaças e seus efeitos que podem colocar em risco o negócio de uma organização.
Fonte: Adaptado de Raggad, (2010).

De referir que, uma organização que não dá tratamento aos riscos inerentes ao seu negócio, a probabilidade de ocorrer um incidente é maior, pois o risco de sofrer um ataque é grande, uma vez que não há nenhum procedimento de prevenção contra ameaças existentes. Uma ameaça ao realizar um ataque, causa incidente que pode provocar impacto negativo no negócio. Assim, para impedir que ameaças explorem vulnerabilidades, faz-se necessário a organização manter um controlo eficaz dos riscos, através da implementação das seguintes medidas de proteção, de acordo com Sêmola (2003):

- **Medidas preventivas** – são controlos implementados numa organização para proteger-se de todas as adversidades e perdas, de modo a evitar que incidentes venham a ocorrer. São medidas que devem ser aplicadas em todas as áreas em que o risco não é aceitável. Abaixo, alguns exemplos:

  - Política de segurança;
  - Instruções e procedimentos de trabalho;
  - Campanhas de formação e sensibilização de utilizadores; etc.

- **Medidas de detecção** – visam identificar elementos causadores de ameaças, como as pessoas , a fim de evitar que os mesmos explorem vulnerabilidades. Essas medidas ajudam a reduzir as vulnerabilidades e assim, impedir que um dano se concretize. Exemplos:

  - análise de riscos
  - sistemas de detecção de intrusão;
  - câmeras de vigilância; etc.

- **Medidas de correção**: são medidas que visam reduzir o impacto de um ataque ou incidente. Exemplos:

  - restauração de *backup* ou de serviços;
  - plano de continuidade de negócios e;
  - plano de recuperação de desastres.

"Um exemplo de medidas de protecção que reduz a probabilidade de uma ameaça se concretizar seria a mudança de um data center (alvo) de uma localidade com registro de

ocorrência frequente de enchentes (ameaça) para outra com probabilidade menor de excesso de chuva" (Beal, 2005, p. 27).

Wheeler (2011), alerta que, uma medida preventiva pode alterar a probabilidade de uma vulnerabilidade ser explorada por uma ameaça, mas nada faria para mudar a gravidade que ocorreria se a ação fosse consumada. Assim como uma medida corretiva não pode diminuir a probabilidade de ameaças explorarem vulnerabilidades, mas uma vez, que a ameaça é detectada, pode limitar o impacto que podia provocar, ao reduzir o seu campo de ação. Já a medida de detecção pode ter o efeito de um impedimento que reduz a probabilidade de vulnerabilidades serem exploradas. Geralmente limita o impacto que poderia causar com a exploração, permitindo a organização responder rapidamente ao ataque.

Entre outros conceitos de interesse na gestão de riscos, conforme Sêmola (2003) e Beal (2005), temos:

- **Impacto** – refere-se ao efeito ou consequência dos danos causados por um ataque ou incidente sobre os processos de negócio;
- **Ataque** – evento que ocorre da exploração de uma vulnerabilidade por uma ameaça. Exemplo: inserção de dados incorretos por um utilizador.
- **Incidente** – é um evento não desejado que pode comprometer o negócio de uma organização, através de resultados negativos, consequentes de um ataque bem sucedido. Exemplo: "pagamento indevido em decorrência da inclusão indevida de fatura de compra no sistema" (Beal, 2005 p. 15).

2.2.3.1 Principais Ameaças à Segurança da Informação

Os avanços tecnológicos fazem com que as PME´s dependam cada vez mais da TI. Com esta dependência, as informações ficam mais expostas aos riscos. Daí, a necessidade das organizações, investirem em recursos adequados para a proteção da informação existente nestes ambientes por ter valor e apresentar sensibilidades. No caso de uma rede interna (empresa) ou externa (internet), as informações que aí trafegam estão expostas a uma variedade de tentativas de ataque, que se forem bem sucedidas podem provocar prejuízos ao negócio. Os riscos podem ser provocados por ameaças, como os vírus, por estarem relacionados com o uso constante das tecnologias da informação nas empresas.

As ameaças como *vírus, cavalos de tróia, adware, spyware, backdoors, worms, bots, botnets, rootkits e spam,* são chamadas de código malicioso. E são aqui, realçadas, por serem as mais comuns.

2.2.4 Código Malicioso

Código malicioso (malware[5]) é um termo genérico, atribuído a qualquer tipo de *software* ou programa, intencionalmente desenvolvido para executar ações não desejadas ou impedir o funcionamento normal de um computador ou sistema (Erbschloe, 2005).

Para Peltier (2005), o envio de *e-mail,* é um dos métodos mais eficazes para introduzir código malicioso no sistema de rede de uma organização.

Abaixo, breve apresentação descritiva dos principais programas maliciosos:

Vírus - é um programa malicioso que inicia uma acção num computador sem o consentimento do utilizador que, ao se propagar, infeta outras aplicações existentes. Um vírus para se tornar ativo e iniciar o processo de infeção, requer a intervenção do utilizador para execução do ficheiro ou programa malicioso. Este processo, pode ocorrer de várias formas:

- Abrir e-mail com anexos;
- Abrir aplicativos de textos, folha de cálculo, etc.;
- Através de partilha de informações, etc..

***Worm* –** O *worm* é diferente do vírus, por ser um programa capaz de se propagar automaticamente para outros computadores numa rede, seja por via da internet ou por uma rede local, sem necessidade de interação com o utilizador.

Mas, como o *worm* é criado para contaminar o máximo de computadores possível, com o envio de cópias de si mesmo, qualquer meio para o efeito é aceitável, como a intervenção de um utilizador para a propagação.

Cavalo de Tróia – é um programa malicioso que faz-se passar por um aplicativo útil, mas que na realidade cria condições para que um *hacker* possa remotamente ter acesso aos ficheiros do computador infetado e realizar as seguintes ações:

[5] *Malware*, do inglês *malicious code* é um termo genérico usado para se referir aos programas que executam ações maliciosas.

- Remoção de ficheiros do computador infetado;
- Roubo de senhas e outras informações confidenciais;
- Renomeação de ficheiros;
- Alteração das configurações do computador e;
- Alteração ou destruição de ficheiros.

Adware **-** é um programa projectado especificamente para exibir publicidade não desejada, quer através de janelas novas (*pop up*), quer através de um outro programa instalado em outro computador.

Spyware – é um programa instalado num computador sem a permissão do utilizador com objetivo de espionar as suas atividades e capturar informações sensíveis sobre ele para posteriormente serem enviadas à outros, via internet.

O *spyware* é uma ferramenta como muitas outras, utilizada para roubo de identidade, que é um risco enorme para aqueles que navegam em redes inseguras ou pública como a internete.

Backdoors **-** é uma ferramenta maliciosa que é incluída através da ação de outros códigos maliciosos ou por atacantes que exploram vulnerabilidades existentes nos programas instalados num computador para invadí-los. Permitindo, assim, que um invasor retorne a um computador infectado sem ser notado. O invasor ao aceder remotamente, o backdoor permite-lhe que se conecte ao sistema. Este é o tipo mais comum de funcionalidade do *backdoor*.

Bot **–** é um aplicativo que dispõe de mecanismos de comunicação com o invasor, permitindo que seja controlado remotamente. O seu processo de infecção e propagação é similar ao *worm*, capaz de se propagar automaticamente, explorando vulnerabilidades existentes em *softwares* ou programas instalados em computadores.

Ao comunicar-se através de um servidor *web*, o invasor pode ter controlo sobre o computador infectado pelo *bot*, enviando instruções para realizar ações perigosas, como desferir ataques, furtar dados, enviar *spam* e *phishing*.[6]

Botnet - é uma rede de computadores infectados por bots. Normalmente são centenas e milhares de computadores ligados com bots, ficando estes a disposição do atacante para o

[6] Método de envio de correio electrónico, usado por um fraudador com objectivo de tentar obter dados pessoais, como número de cartões de crédito a fim de realizar um furto.

envio de comandos para realizar ações perigosas como ataques de negação de serviço ou propagação de códigos maliciosos.

Rootkit **-** é um conjunto de programas e técnicas que permite ocultar e assegurar a presença de um atacante num computador invadido. Isto, significa que, com a instalação do programa, o invasor facilmente terá acesso ao computador comprometido sem ter que recorrer a outros procedimentos.

Spam - refere-se aos e-mails enviados à um grande número de pessoas sem terem sido solicitados, como por exemplo, conteúdo publicitário enganoso. Muitos invasores utilizam-se de spam para a disseminação de códigos maliciosos e venda ilícita de produtos.

Engenharia social é outro tipo de ameaça que deve ser observada, além das ameaças descritas atrás, por tratar-se de um método de ataque utilizado por alguém, como o uso da persuasão, com objetivo de obter acesso não autorizado à dados importantes e sensíveis de uma organização.

2.2.5 Engenharia Social

Grande parte das informações, aparentemente inócua, na posse de uma empresa é valorizada por um atacante de engenharia social, porque pode desempenhar um papel vital em seu esforço para vestir-se com um manto de credibilidade[7] (Mitnik & Simons, 2003).

O uso de habilidades sociais para convencer as pessoas a revelar senhas de acesso ou outras informações valiosas é chamado de engenharia social (Witman & Mattord, 2010).

Para Mitnick (2003), engenharia social é a habilidade que um *hacker* possui em manipular pessoas para obter informações necessárias para conseguir acesso não autorizado a um sistema.

Na visão de Witman e Mattord, (2009), *hacker* é aquele individuo que usa métodos deliberados como *softwares* para obter acesso a informação de forma ílicita e realizar ações de espionagem ou transgressões.

[7] Depreende-se que o atacante pode fazer-se passar por um profissional confiável da empresa, em que, a pretexto de uma atualização de dados de caráter urgente, envia mensagens de correio eletrónico, com o objetivo de obter dados pessoais do destinatário e posterior realização fraudulenta.

Engenharia social pode acontecer de várias formas, como alguém que, aproveitando-se da confiança ou ingenuidade de outra pessoa, tenta persuadi-la à fornecer informações e até mesmo senhas de acesso para depois realizar ações criminosas, como furto de informações, etc.

Abaixo, alguns exemplos de métodos de ataque de engenharia social:

- contacto telefónico para dissimular um pedido razoável e assim explorar a vítima para realizar os seus objetivos;
- intranet refere aos funcionários descontentes que podem aceder ao sistema da empresa a partir de fora e passarem por outra pessoa;
- contacto através de e-mail mostrando interesse num assunto específico do conhecimento da vítima ou por *phishing*, nome dado a uma mensagem que contém marcas comerciais, endereços de *e-mail* e links forjados que aparentam proceder de um banco ou de uma outra empresa com o objetivo de recolher dados financeiros de clientes.

Como visto anteriormente, a informação numa organização é sem dúvida, o recurso disponível mais valioso. Ele é o principal recurso utilizado para gerar continuamente valor ao negócio em toda a organização. Qualquer ameaça aos ativos de informação é uma ameaça direta à capacidade da organização gerar valor ao negócio. Assim, aplicar medidas de proteção adequadas contra as ameaças no seu ambiente e consciencializar os seus funcionários a terem procedimentos corretos no uso da internet,[8] faz parte de uma gestão eficaz dos riscos de segurança que uma organização enfrenta.

2.2.6 Mecanismos de Proteção

Existem diversos mecanismos que podem ajudar uma empresa a manter-se protegida contra os vários tipos de ameaças no seu ambiente, como:

- **Política de Segurança da informação** - é um documento importante concebido por uma organização para proteger-se das ameaças impostas à segurança da informação. Estabelece diretrizes, normas, procedimentos e instruções, de modo, a responsabilizar

[8] Ajuda a evitar fraudes que são movidas por fontes ilícitas, que se aproveitam de alguma fragilidade, utilizando os seus computadores para realizarem atividades de má-fé.

todos os colaboradores ou utilizadores pela proteção da informação que usam. A política deve estar em conformidade com requisitos legais, pelo que deve ser respeitada, estipulando sanções em caso de incumprimento desta;

- ***Firewall*** - é uma barreira de segurança que consiste em proteger uma rede interna ou local contra eventuais violações por parte de uma rede externa não segura como a internet, impedindo o acesso não autorizado que ocorra de fora da rede. Ele filtra a informação, permitindo somente a passagem de informações legítimas.

- **Plano de Continuidade de negócio** - visa garantir a continuidade ou recuperação de processos e informações críticas relevantes á organização, com o objetivo de minimizar o impacto decorrente de efeitos de falhas ou desastres significativos que não foi possível ser evitado.

- ***Backup*** - refere-se a cópias de segurança de informações relevantes para a organização para posterior recuperaração em caso de um incidente. As cópias devem ser feitas em mídias e mantidas em locais seguros. O *Backup* deve ser sempre atualizado.

- **Antivírus** - considerado como uma ferramenta anti-malware, são programas concebidos para detectar e remover vírus em computadores.

- **Criptografia** - é a arte de escrever mensagens em forma cifrada ou em código, usado para proteger informações essenciais ou proteger-se dos riscos associados ao uso da internet.

É importante realçar, que não bastam os recursos mencionados acima para resolver os problemas de ataques. Uma boa segurança não se inicia nem termina com a instalação de firewalls e antivírus.[9] Ela (segurança da informação), só é adequada, se estiver alinhada com os objectivos e metas da organização. Os Gestores precisam entender a problemática da segurança, como a segurança afeta a organização e os seus clientes, para que sejam disponibilizados os recursos, tempo e financiamentos necessários. Por outras palavras, a segurança da informação deve ser aplicada através de uma abordagem hierárquica *top-down*

[9] Uma boa segurança deve ser planeada, desenhada, implementada, mantida e ter capacidade para evoluir. Necessitando deste modo, de uma abordagem de gestão para que sejam considerados todos os aspectos relacionados com os objetivos estratégicos de segurança e do negócio.

(de cima para baixo). Pois que, a sua implementaçao na empresa, só será, bem sucedida, se houver comprometimento por parte da administração de topo, isto é, deve haver um envolvimento claro e inequívoco por parte daqueles que têm poder de decisão.

Outro recurso importante na proteção da informação é a classificação da informação, por ser uma medida de prevenção que pode ajudar a minimizar os riscos (ISO/IEC 27005[10]:2008).

2.2.7 Classificação da Informação

As organizações classificam as informações para estabelecer níveis de protecção adequados ao valor que possui para o negócio. Como os recursos são limitados, é necessário identificar e priorizar àquelas que realmente necessitam de proteção, pois as informações podem ser criadas da mesma forma, mas nem todas têm o mesmo valor para a organização (Peltier, 2011).

Conforme a ISO/IEC 27005:2008, a informação pode ser classificada em:

- **Pública** – informação que pode ser disponibilizada ao público através de canais autorizados pela empresa e que não causam consequências graves ao funcionamento normal da empresa. A integridade desse tipo de informação não é vital;
- **Interna** – informação usada por todos os funcionários para a realização das atividades e condução dos negócios da empresa. Esse tipo de informação não é vital para a organização mas a sua integridade é importante;
- **Confidencial** – informação sensível da empresa que se for divulgada pode causar perda de privacidade, quebra de equilíbrio funcional, danos à imagem da empresa perante o cliente e reduzir assim a vantagem competitiva, permitindo ao concorrente tirar vantagem expressiva;
- **Secreta** – informação crítica para as atividades da empresa que se for divulgada pode causar impacto na vantagem competitiva da empresa ou nas suas estratégias de negócio. A integridade da informação deve ser rigorosamente preservada e o acesso deve ser restrito apenas à algumas pessoas. O manuseamento de informação secreta é vital para a organização.

[10] Norma internacional que visa disponibilizar orientações para a gestão de risco de segurança da informação.

Conforme mencionado atrás, pode-se seguramente, dizer, que cada organização é quem define o grau de importância que tem a informação usada no negócio e por esta razão deve capacitar e sensibilizar os seus funcionários a fazerem uso adequado das informações em sua posse, pois grande parte dos problemas de segurança, tem a sua origem na própria rede da empresa. Assim, todo funcionário com acesso a informação considerada sensível e privilegiada deve ser monitorizado para uma eventual penalização, se houver violação ou uso não adequado deste recurso.

Sendo a informação um ativo ou um bem valioso para uma empresa, à sua proteção deve fazer parte da estratégia do negócio da organização, e não ser aclamada apenas como uma questão ligada à área de tecnologia de informação.[11] Neste contexto**,** a gestão da segurança da informação, apresenta-se como uma ferramenta de grande valor para qualquer empresa, pois ajuda a manter o funcionamento normal das suas atividades, diante de uma situação de risco ou incidente de segurança.

2.3 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A Gestão da Segurança da Informação aponta para a adoção de medidas de segurança alinhadas com as estratégias de negócio da organização, através da verificação contínua dos processos. Consiste na aplicação de métodos que visam evitar o acesso indevido às informações, tornar menos intenso os riscos seguindo os princípios de segurança da informação "confidencialidade, integridade e disponibilidade" (Wikepédia, 2013).

A GSI, tem como foco principal as características humanas, organizacionais e estratégicas relativas à segurança da informação.

Neste sentido, conforme Beal, (2005, p. 37):

"A adoção de um modelo corporativo de gestão de segurança da informação permite à organização equacionar os desafios de proteção da informação levando em conta todos os aspetos essenciais para a segurança: componentes dos ambientes físico e lógico, pessoas, processos".

[11] Importa referir que a organização deve, atendendo as constantes ameaças no seu ambiente, devido ao uso da TI, alinhar o seu processo de segurança da informação aos seus objetivos de negócio, pois ter uma visão estratégica ou uma abordagem de gestão quanto a SI, contribui para vantagem competitiva.

A prática da Gestão de Segurança da Informação numa empresa, faz com que as decisões e ações relativas a segurança da informação estejam alinhadas aos objetivos e estratégias do negócio da organização. Manter segura as informações relevantes para o sucesso do negócio exige conhecimento. E a norma ISO/IEC 27001, conhecida como norma internacional de segurança, provê as bases fundamentais para que as empresas possam de acordo as suas necessidades, construirem um sistema de gestão de segurança da informação. Um sistema de gestão de segurança da informação, é um veículo a que se pode guiar, pois ajuda a manter assegurada as informações cruciais para o negócio da organização, através de práticas e procedimentos que atendem aos objetivos de segurança da organização.

2.3.1 Sistema de Gestão da Segurança da Informação

Um sistema de gestão de segurança da informação é a parte do sistema global de gestão, baseado numa abordagem de risco, que permite definir, implementar, operaracionalizar, monitorizar, manter e melhorar as boas práticas de segurança da informação (BS ISO/IEC 27001:2005).

Segundo Raggad (2010), um SGSI[12] é uma estrutura de segurança adotada para gerir a segurança da informação com base numa abordagem de risco, para estabelecer e manter segura as informações de negócio de uma empresa. Ainda de acordo com o autor, o desenvolvimento de um sistema de gestão de segurança da informação numa organização, depende do contexto do risco do negócio da organização. Isto implica que determinados fatores devem ser considerados na implementação de um sistema de gestão de segurança da informação.[13]

Qualquer segurança da informação deve ser planeado, implementado e mantido. Neste âmbito, o SGSI deve garantir que os controlos desenvolvidos servirão para fornecer segurança da informação adequada e satisfatória às especificações exigidas pelos utilizadores, clientes e parceiros de negócios. Um SGSI que está em conformidade com a norma ISO 27001 é importante, pois permite demonstrar aos parceiros comerciais e clientes que a

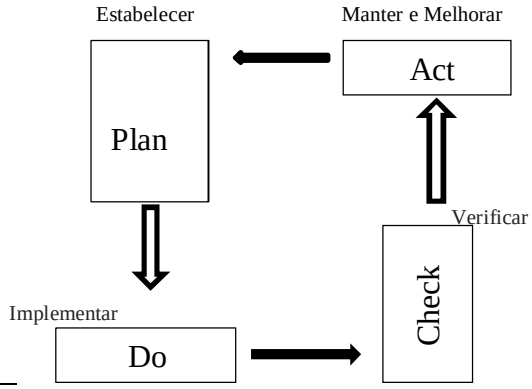
[12] Sistema de gestão de Segurança da informação. Considerado como o método mais importante para soluções de segurança da informação por dispor de elementos fundamentais que podem ajudar uma empresa a proteger e manter um ambiente seguro para as informações (Raggad, 2010).
[13] A implementação de um SGSI depende das necessidades, do tamanho e estrutura da organização. Portanto a organização precisa especificar as suas necessidades e objetivos de segurança.

empresa não só protege adequadamente as informações da organização, como também as suas informações[14] (Raggad, 2010).

Para a construção de um Sistema de Gestão da Segurança da Informação, a norma ISO/IEC 27001, exige que se adote o modelo PDCA. O PDCA[15] que significa *plan, do, check, act,* é um " *(...) método utilizado em processos de gestão da qualidade que se aplica aos mais diversos tipos e níveis de gestão, é útil para fornecer uma visualização global das etapas que devem compor a gestão da segurança da informação*" (Beal, 2005, p. 37).

De acordo com Raggad (2010), o SGSI é desenvolvido por meio de quatro fases fornecidos pelo modelo PDCA que são:

- Plan (fase planear) estabelece a política do SGSI, os objetivos e processos como a abordagem da avaliação de risco da organização e seleção dos objetivos de controlo e controlos para o tratamento de riscos;
- Do (fase fazer) implementar e operar a política do SGSI, plano de tratamento de risco, controlos e medir a eficácia dos controlos implementados; crédito
- Check (fase verificar) acompanhar e analisar o SGSI, fazer monitoramento e revisão por formas a avaliar e medir a eficácia dos controlos implementados em relação a política e/ou os objetivos do SGSI;
- Act (fase agir) manter e melhorar o SGSI. Tomar ações corretivas e preventivas adequadas com base nos resultados da realização de controlo interno para garantirem melhoria contínua do SGSI.



[14] Salienta-se, que o fato de uma empresa ter implementado no seu ambiente de negócios requisitos de segurança da informação em conformidade com as políticas e normas internacionais não implica que esteja 100% seguro ou que os clientes e parceiros se sintam totalmente protegido de qualquer risco. Um SGSI ajuda sim, na reputação e credibilidade de negócios por prover métodos eficazes que permite reduzir os riscos e manter os níveis adequados de segurança.

[15] Termo em inglês que significa *Plan, Do, Check, Act* (planear, implementar, analisar, manter e melhorar um sistema de gestão da segurança da informação).

Figura 4 - Modelo PDCA para o desenvolvimento de um SGSI
Fonte: Adaptado de Raggad (2010)

Para o planeamento do projecto SGSI, a norma ISO/IEC 27001 descreve os seguintes passos:

1. definição do escopo do SGSI;
2. definição de uma política de segurança;
3. realizar uma avaliação/análise de risco;
4. gestão de risco;
5. selecionar objetivos de controlo e controlos reais a serem implementadas ou aplicadas;
6. preparar uma Declaração de Aplicabilidade.

A adoção de um SGSI deve ser uma decisão estratégica para uma organização.[16] Um sistema de gestão de segurança da informação para ser eficaz na sua implementação requer o comprometimento da gestão de topo, por ser o elemento imprescindível na tomada de decisão para a implementação formal do SGSI. É importante que a administração de topo se envolva de fato nesse compromisso. Pois, conforme a NP ISO/IEC 27001 (2013), ao estabelecer, implementar, manter e melhorar de forma contínua um sistema de segurança da informação, a gestão de topo deve demonstrar liderança e comprometimento para com o SGSI através do seguinte:

a) assegurar o estabelecimento da política de segurança compatível com a estratégia da organização;

b) assegurar que os objetivos do sistema de gestão da segurança da informação são integrados nos processos organizacionais;

c) assegurar que os recursos para o SGSI estão disponíveis;

d) comunicação da importância de um SGSI para a organização;

e) assegurar que os resultados pretendidos são alcançados com o SGSI;

[16] A gestão de segurança da informação deve ser vista como parte integrante dos objectivos estratégicos de negócio de uma organização. A administração ao alinhar a segurança às suas estratégias de negócio, demonstra interesse na eficácia da implementação de um sistema de gestão de segurança da informação. O risco de segurança pode afectar o negócio e causar algum impacto de maior ou menor proporção, tornando a organização menos competitiva se não forem definidos programas de gestão de risco.

f) orientando e apoiando as pessoas de modo a contribuir para a eficácia do sistema de gestão da segurança da informação;

g) promovendo a melhoria contínua;

h) apoiando outras funções de gestão relevantes a demostrarem a sua liderança, conforme aplicável às suas áreas de responsabilidade.

No que toca a participação efetiva da alta direção, os pontos mencionados acima são elucidativos, pois somente com o apoio desta se torna possivel implementar um sistema de gestão da segurança da informação. Muitas empresas privam-se da implementação desses processos por desconhecimento ou por acharem os seus custos elevados, mas não fazem ideia do quanto perdem com a não adoção do sistema de gestão de segurança da informação. Um SGSI é sistematicamente importante, pois está voltado para operar na gestão de segurança da informação de qualquer organização, definindo programa de segurança de risco apropriado para corrigir inconformidades e prevenir incidentes de segurança indesejados. Uma organização que tenha implementado um SGSI no seu negócio, garante melhoria satisfatória à confidencialidade, integridade e disponibilidade de seus ativos de informações.

Importa, realçar que, para uma empresa ter uma segurança considerada aceitável, precisa ter uma boa política de segurança, composta de normas claras, aplicáveis e alinhada com os objectivos de negócio da empresa. O envolvimento de todos contribui para a materialização satisfatória da segurança. Mas atenção que, o importante não é apenas proteger as informações confidenciais, é necessário sensibilizar as pessoas que as usam, através de programas de consciencialização. E a política de segurança da informação deve abordar estes aspectos.

2.3.2 Política de Segurança da Informação

A medida que as tecnologias de informação se fazem cada vez mais necessárias às empresas, torna-se imprescindível a criação e manutenção de uma política que mantenha a informação íntegra, disponível e acessível a todos que estejam devidamente autorizados.

> "Por política de segurança entende-se política elaborada, implantada e em contínuo processo de revisão, válida para toda a organização, com regras o mais claras e simples possível e estrutura gerencial e material de suporte a essa política, claramente sustentada pela alta hierarquia" (Caruso & Sttefen, 1999, p. 24)

Uma política de Segurança da Informação deve ser elaborada de acordo com os objectivos de segurança da empresa e ser revista periodicamente para manter sempre actualizada. Mas para o efeito, necessita do envolvimento da administração da empresa, como órgão competente para aprovar a PSI,[17] pois só deste modo, é que as regras que forem estabelecidas na política serão divulgadas e cumpridas por todos na empresa.

E Beal (2005) é clara ao afirmar que uma política de segurança da informação deve ser aprovada a nível superior hierárquico da empresa para que fique evidente a responsabilidade da direção com as metas e princípios de segurança da informação estabelecidos.

A política de segurança é um documento indispensável para a proteção da informação contra as ameaças à segurança da informação. Uma empresa, ciente da importância que tem uma política de segurança da informação, deve implementar, pois visa preservar o valor do ativo e diminuir os riscos inerentes ao seu uso.

Mas, é importante, observar que, de acordo com Caruso & Sttefen (1999, p. 24):

"Não existe política de segurança certa ou errada; não há política de segurança pronta para uso. Cada empresa deve ter uma solução única e adequada para o seu caso, para a sua cultura".

Caruso e Steffen (1999, p. 49) declaram que "As consequências de uma política de segurança implementada e corretamente seguida podem ser resumidas em três aspetos:"

- redução da probabilidade da ocorrência;
- redução dos danos provocados por eventuais ocorrências;
- criação de procedimentos para se recuperar de eventuais danos.

Referindo-se aos três aspetos, citados acima, os mesmos autores explicam que uma política de segurança da informação, é uma medida de carácter preventivo, pois os riscos devem ser previstos e eliminados antes que se manisfestem. Até porque os custos com a prevenção podem ser menores do que a restauração dos danos causados por falta de segurança. Mas, se ocorrer, algum incidente, apesar das medidas de prevenção, os danos causados devem ser reduzidos ao mínimo. Mas, se mesmo com todas as precauções tomadas,

[17] Além de aprovar a política de segurança da informação, a administração deve definir uma área responsável pela segurança da informação de acordo com a necessidade de gestão da segurança e do negócio.

vier a ocorrer um incidente, é necessário que se estabeleça um plano para se recuperar dos danos provocados pelo incidente.

Uma política de segurança da informação contribui para o processo de educação dos funcionários (utilizadores) de uma empresa. Ela é elaborada através de normas internacionais que provê informações de gestão para as melhores práticas de segurança da informação.

2.4 NORMAS DE SEGURANÇA DA INFORMAÇÃO

A necessidade de se preservar a confidencialidade, integridade e disponibilidade das informações fez com que surgissem normas internacionais vocacionadas para auxiliarem as empresas a se protegerem, através de orientação à construção de uma base de segurança da informação comum com o objetivo de reduzir os riscos. Segundo Beal (2005) as normas servem de auxílio às empresas para implementar as melhores práticas da gestão da segurança da informação.

2.4.1 ISO 27001

A ISO/IEC 27001 constitui a base fundamental para as organizações por prover uma abordagem eficaz à gestão da segurança da informação assegurando a proteção da confidencialidade, integridade e disponibilidade das informações através da implementação de controlos adequados. Um modelo ISMS[18] implementado em conformidade com a ISO/IEC 27001 pode ajudar uma empresa a demonstrar boas práticas na gestão da segurança da informação dando indicações aos seus clientes e fornecedores, de que protege adequadamente as suas informações.

O modelo de segurança focado na ISO/IEC 27001, estabelece, implementa, opera, revê, mantém e melhora a segurança da informação. O que quer dizer que a segurança da informação não deve ser planeada, implementada e mantida sem este modelo (Raggad, 2010).

A norma ISO[19]/IEC 27001:2005, foi oficialmente publicada em 15 de Outubro de 2005. Ela anula e substitui a antiga norma Britânica BS 17799-2 (publicada em 2002 pela BSI[20]).

[18] Information Security Management System (Sistema de Gestão de Segurança da Informação).
[19] *International Organization Standardization*. Foi fundada em 1947 em Geneva, Suíça, para desenvolver normas internacionais com o objectivo de auxiliar as empresas.
[20] *British Standards Institution*. É um instituto inglês vocacionado para criação de normas.

Esta norma (ISO 27001) é usada para certificação e pode estar alinhada com outros sistemas de gestão, como a norma ISO 9001(qualidade) e ISO/IEC 20000 (gestão de serviços de TI).

A ISO/IEC 27001, define os requisitos para um SGSI, que são:

- Sistema de Gestão de Segurança da Informação (SGSI);
- Responsabilidade de Gestão;
- Auditorias internas do SGSI;
- Revisão de Gestão do SGSI;
- Aperfeiçoamento do SGSI;
- Objetivos de controlo e controlos.

Não importa o segmento de mercado em que atue uma empresa, assim como seu *core business*[21] e porte. Qualquer empresa (pequena, média ou grande), pode fazer uso da ISO/27001. A implementação da ISO/IEC 27001 numa organização, demonstra a seriedade com que é tratada a gestão da segurança da informação com a aplicação de controlos adequados para proteção da informação, garantindo a continuidade de negócio e redução do impacto procedente de eventuais incidentes de segurança. Ajuda a fornecer a clientes e fornecedores confiança e credibilidade comercial, pois são aplicados processos de segurança para lidar com as ameaças e riscos que causam incidentes de segurança.

A ISO/IEC 27001, usada para certificação[22], interage com a norma ISO/IEC 27002 que é o código de práticas em gestão da segurança da informação.

2.4.2 ISO/IEC 27002

A ISO 27002 é um código de práticas em gestão de segurança da informação que provê orientações gerais sobre os objetivos de segurança da informação aceites internacionalmente. Os objectivos de controlo e controlos presentes na norma são implementados para atenderem aos requisitos identificados através de uma avaliação de riscos. Esta norma pode ser considerada como o ponto de partida para o desenvolvimento de

[21] *Core business* é uma expressão em inglês que significa a parte central de um negócio ou de uma área de negócios ou seja refere-se ao foco principal do negócio de uma determinada organização. Portanto aquele que tem maior peso em termos de facturação.
[22] Esta norma é usada para certificação de empresas que adotam as boas práticas de segurança da informação com a implementação de um sistema de gestão da segurança da informação.

procedimentos específicos de segurança da informação da organização (BS ISO/IEC 27002, 2005).

A ISO 27002 contém 11 seções de controlos de segurança da informação que totalizam, juntas, 39 categorias principais de segurança e uma seção introdutória que aborda a análise/avaliação e o tratamento de risco (BS ISO/IEC 27002:2005). As 11 seções fundamentais da norma são:

1. Política de Segurança da Informação;
2. Organização da Segurança da Informação;
3. Gestão de Activos;
4. Segurança em Recursos Humanos;
5. Segurança Física e do Ambiente;
6. Gestão das Operações e Comunicações;
7. Controlo de Acesso;
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
9. Gestão de Incidentes de Segurança da Informação;
10. Gestão da Continuidade do Negócio;
11. Conformidade.

Abaixo, resumo informativo dos processos de segurança da informação mencionadas acima:

- **Política de Segurança** – o seu objetivo é fornecer orientação e suporte para gestão de segurança da informação de acordo com os requisitos de negócio, assim como as leis e regulamentos pertinentes. A norma diz que uma política de segurança da informação deve ser clara e estar alinhada com os objetivos do negócio. Porêm para a sua implementação e manutenção segundo a norma, a administração deve demonstrar o seu apoio e responsabilidade com a segurança da informação. A política de segurança é o documento que declara, por escrito, como a empresa pretende proteger os seus ativos[23], como pretende educar os seus funcionários (utilizadores) e como as medidas de segurança serão realizadas e cumpridas.

[23] Refere-se a proteção dos ativos da informação.

- **Organização da Segurança da Informação** – Com relação a este ponto, o seu objetivo é mostrar como a organização deve internamente gerir a segurança da informação. A norma diz que o controlo e implementação da segurança da informação dentro da organização, deve ser definido a partir de um quadro de gestão. Portanto, este ponto enfatiza a necessidade de uma estrutura de gestão de segurança da informação. Assim, a administração de topo deve definir uma estratégia global e aprovar os princípios de segurança da informação, delegar responsabilidades, coordenar e revêr a implementação da segurança em toda a organização. Dependendo do tamanho da organização, tais responsabilidades podem estar a cargo de especialistas internos afetos à gestão ou especialistas externos ou mesmo por um conselho de administração. O primeiro ponto a ser aprovado é a política de segurança da informação que tem a função de informar os colaboradores dos requisitos obrigatórios para proteger os ativos de informação. A norma recomenda que a política deve especificar os mecanismos que através dos quais estes requisitos podem ser atendidos. Portanto, a utlização de ferramentas de segurança devem estar alinhadas com a política de segurança da informação.

- **Gestão de ativos** – este objetivo de segurança informa que os ativos de informação têm diferentes sensibilidades e disponibilidades e portanto requerem diferentes tipos de proteção. Segundo a norma ISO/IEC 27002:2005 a gestão de ativos engloba a informação (base de dados, contratos e acordos, documentação do sistema, etc.); software (aplicações,) e ativos físicos (equipamentos de informática e de comunicações). A norma diz que há dois elementos fundamentais na gestão de ativos que são:

    1. Responsabilidade pelos ativos;
    2. Classificação da informação.

No que concerne o primeiro ponto, a norma diz que a organização deve identificar todos os ativos e designar responsáveis pelos mesmos. A norma descreve o inventário de ativos como atividade principal relacionada com a responsabilidade pelos ativos incluindo o tipo de activo, formato, localização, informações de *backup*, o valor de ativo, etc. O inventário de activos ajuda a garantir que a protecção dos mesmos, ocorra de maneira eficaz. O inventário de ativos é também um importante pré-requisito para a gestão de risco.

Em relação ao segundo ponto, a classificação da informação é o método que ajuda a organização a determinar como a informação deve ser tratada e protegida.

Outro objetivo de segurança a ter em conta é a segurança em recursos humanos, pois segundo Beal (2005), "*Apesar da maior atenção concedida pela mídia aos ataques causado por hackers, estudos demonstram que grande parte dos incidentes de segurança é provocada por integrantes da própria organização (…)*".

- **Segurança em Recursos Humanos** – visa minimizar os riscos de segurança atribuídas a recursos humanos. Os incidentes incluem, por exemplo, os erros humanos, fraude, abuso, mau uso, etc. Esses aspetos devem ser considerados no ato da contratação para evitar que os mesmos ocorram. Desta forma, a melhor prática conhecida para a segurança em recursos humanos, pode ser a formação e sensibilização para todos os utilizadores e funcionários. Como diz a norma, deve existir um programa regular de sensibilização sobre a segurança da informação a fim de tornar os funcionários e entidades externas conscientes das suas responsabilidades de segurança. A norma recomenda que o programa de sensibilização deve estar de acordo com a política de segurança da informação e com os procedimentos pertinentes em consideração a informação a ser protegida.

De acordo com a norma ISO/IEC 27001, o processo disciplinar, é outro elemento fundamental na segurança em recursos humanos. Uma punição é importante para ajudar a evitar que funcionários e colaboradores de entidades externas violem a política de segurança da informação.

Um dos aspetos importantes na gestão da segurança da informação é a proteção do ambiente e dos ativos físicos da organização.

- **Segurança Física e Ambiental** – De acordo com a norma BS ISO/IEC 27002 o objetivo da segurança física e ambiental é de prevenir o acesso físico não autorizado, assim como danos que possam ocorrer numa empresa, evitando a perda, dano, roubo de activos e interrupção das atividades.

O objectivo de segurança física e ambiental propõe duas práticas de segurança como segue:

- Áreas seguras e;

- Segurança de equipamentos.

Com relação a prática de segurança, áreas seguras, a norma recomenda que os perímetros de segurança física devem ser considerados e implementados, quando apropriado, para salvaguardar a informação da empresa. Para se ter áreas seguras, de acordo a norma, a organização deve criar uma área de recepção que permita o acompanhamento de forma presencial assim como controlos de entrada física para controlar o acesso físico as instalações, como os cartões de acesso. Recomenda também o uso de sistemas de vigilância e de alerta, incluindo detectores de intrusão e câmeras. Portanto o acesso aos Centros de Processamento de Dados e Zonas Críticas deve ser restrito apenas às pessoas autorizadas;

Quanto a segurança de equipamentos, a norma recomenda que a instalação de equipamentos de processamento de informação que lidam com dados sensíveis devem ser colocados em locais seguros de formas a reduzir o risco de visualização por pessoas não autorizadas.

O acesso á informação numa organização deve obedecer a determinados padrões, que são estipulados para a proteção da informação. E o controlo de acesso é uma prática de segurança fundamental na proteção da confidencialidade, integridade e disponibilidade da informação.

- **Controlo de Acesso** – o seu objetivo é controlar o acesso a informação. A norma diz que o acesso à informação, as instalações de processamento da informação e processos de negócio, devem obedecer a regras de controlo de acesso definidas numa política de autorização e divulgação da informação baseada em requisitos de negócios e de segurança.

Segundo a norma o controlo de acesso é lógico e físico, devendo serem considerados em conjunto. Todos os funcionários e prestadores de serviços devem ter uma noção clara dos requisitos de negócios a serem cumpridos. Assim segundo a norma, a política de controlo de acesso deve ter em conta os requisitos de segurança de aplicações de negócios, políticas de divulgação de informações e acesso à mesma. A norma recomenda também, o uso de procedimentos de *login*[24] seguros, pois uma técnica de autenticação adequada deve ser

[24] Termo em inglês que define o processo de acesso a um sistema através da identificação e autenticação do utilizador. Por questões de segurança, um *login* deve ser único para cada utilizador, isto é, ser reconhecido pelo nome de identificação e por uma senha (palavra-passe).

escolhida para comprovar a identidade de um funcionário. Os acessos devem ser concedidos e autorizados mediante um pedido formal de acesso.

É recomendada a criação de uma matriz de acessos alinhada com a política de controlo de acessos para serem definidas restrições de acessos e assim controlar ou definir os dados que podem ser acedidos por um funcionário em particular.

- **Gestão das Operações e Comunicações - e**sta é uma área de grande importância para a segurança da informação. Segundo a norma ISO/IEC 27002, visa garantir a segurança e uma operação segura e correta dos recursos de processamento de informação assim como estabelecer controlos para garantir a segurança da comunicação bem como assegurar que a segurança das comunicações é analisada. Estas recomendações estão divididas em 10 práticas de segurança como segue:

  - Procedimentos e responsabilidades operacionais;
  - Gestão de serviços terceirizados;
  - Planeamento e aceitação de sistemas;
  - Cópias de segurança;
  - Gestão de segurança em redes;
  - Manuseio de Mídias;
  - Troca de informações;
  - Serviços de comércio eletrónico; e
  - Monitoramento

Cada item mencionado acima, possui vários controlos que devem ser implementados para garantir a segurança da informação. A norma recomenda a atribuição de responsabilidades e procedimentos de gestão de segurança da rede. Diz também ser necessário existir procedimentos documentados para as actividades operacionais associadas às instalações de processamento de informação, como procedimentos de inicializar e desligar os computadores, métodos de *backups*[25], manutenção de equipamentos, manipulação de suportes de dados, etc. As responsabilidades atribuidas devem estar em conformidade com os objetivos de segurança da organização.

[25] Termo em inglês que em informática significa cópia de segurança. É importante que as organizações possuam cópia dos dados contidos num determinado computador ou centro de processamento de dados para posterior restauração se houver perda dos mesmos. A cópia de segurança normalmente é efectuada todos os dias após o encerramento das atividades.

- **Gestão de Incidentes de Segurança da Informação –** processo de segurança que visa assegurar que eventos e incidentes de segurança da informação sejam comunicados, acompanhados e resolvidos em tempo útil. De acordo com a norma, este processo numa organização aplica-se a todos os funcionários, incluindo fornecedores e entidades externas que, no âmbito da sua ação dentro da organização, devem identificar incidentes de segurança e informar ao ponto de contacto.[26] A norma recomenda que sejam atribuídas responsabilidades e procedimentos para melhor gestão dos riscos e incidentes de segurança da informação. Neste sentido, deve ser nomeado um responsável pelo ponto de contacto que estará incumbido de efetuar a monitorização, detecção e análise dos eventos e incidentes de Segurança de informação. Portanto, todos os incidentes identificados, de acordo com a norma devem ser reportados ao ponto de contacto e este deve garantir que todos os incidentes de segurança são registados e analisados para uma recuperação e resolução eficaz e eficiente do incidente.

Situações que podem ser consideradas para a segurança da informação susceptíveis de constituir um incidente de segurança de informação segundo a ISO/IEC 27002 são:

a) Controlo de segurança ineficaz (não existir segurança numa porta, ou encontrar aberta uma porta de uma zona delicada, por exemplo);
b) Violação de integridade, confidencialidade ou disponibilidade de informação;
c) Erros humanos;
d) Não-conformidades com as políticas e processos definidos;
e) Violação das medidas de segurança física;
f) Mudanças nos sistemas informáticos, sem aviso prévio por parte do dono do sistema;
g) Funcionamento anómalo de *software* ou *hardware*;
h) Violações de acesso a zonas restritas.

- **Gestão da Continuidade de Negócio –** esta seção cuida da continuidade do negócio. A norma ISO/IEC 27002 recomenda a criação de um plano de continuidade de negócios que descreve os processos e procedimentos que uma organização necessita implementar para garantir a continuidade das atividades durante e após um incidente. Portanto um plano de continuidade de negócios, de acordo com a ISO/IEC 27002, impede que haja interrupção das atividades do negócio e protege os processos críticos

[26] Elemento a quem são endereçados todos os eventos e incidentes de segurança da informação.

de segurança, contra efeitos de falhas ou desastres significativos, e assegura a sua reposição em tempo útil.

- **Conformidade –** esta prática de segurança segundo a norma tem haver com critérios que devem ser estabelecidos e cumpridos na organização para evitar a violação de obrigações legais, estatutárias, regulamentares ou contratuais relativas a segurança da informação. A norma recomenda que é necessário haver auditorias periódicas para verificar se todos os critérios e padrões estabelecidos, conforme exigido pela política de segurança da informação estão a ser cumpridos.

2.5 A TI E AS PEQUENAS E MÉDIAS EMPRESAS

A Tecnologia de Informação pode ser vista como um percurso necessário à seguir pelas empresas por prover uma variedade de recursos que servem de sustentabilidade para realizarem os seus negócios. A informação como ativo mais valioso, representa um diferencial competitivo de grande importância estratégica para as organizações. Neste sentido, os recursos de TI são de importância crucial para as pequenas e médias empresas, pois grande parte das informações encontram-se armazenadas em recursos de informação como o computador que é seguramente o pricipal recurso para o processamento de dados. A TI apoia as PME´s nas suas atividades imprimindo maior rapidez na execução do seu processo de negócio e também na tomada de decisão, contribuindo deste modo para o alcance dos seus objetivos estratégicos. Tendo em conta a dependência cada vez maior na tecnologia de informação é importante que as PME´s se consciencializem de que o uso da TI acarreta riscos que podem ser prejudiciais para o seu negócio. Assim, para assegurar o negócio, as empresas devem adotar a gestão da segurança da informação como meio apropriado para controlar os riscos inerentes. Atualmente a segurança da informação não se resume somente em aspetos tecnológicos, ela é abrangente, pois são considerados todos os aspetos relacionados com a segurança da informação. E por esta razão deve ser tratada como um processo e não como um projeto.

É evidente que, para as pequenas empresas, os recursos que detêm são limitados em relação as grandes empresas por não disporem de meios financeiros que lhes permite adquirir tecnologias mais aperfeiçoadas.

Em Angola, os primeiros passos na busca da tecnologia de informação, ocorreram nos finais da década de 80, através de algumas instituições do estado, únicos órgãos que tinham acesso a esse recurso. A partir dos anos 90 e com a liberação do mercado, foram surgindo algumas empresas privadas dos mais variados ramos que foram adquirindo determinados meios como computador (PC), impressoras, etc.

2.6 CONTEXTO DE PEQUENAS E MÉDIAS EMPRESAS ANGOLANAS

Tratando-se de Pequenas e Médias Empresas, inicialmente é importante conhecer como se encontram classificadas. O porte ou tamanho de uma empresa em Angola está definida na Lei n.º 30/11, publicada em Setembro no Diário da República, que regula o novo regime das Micro, Pequenas e Médias Empresas (MPME)[27]. Conforme o *site* da ANIP[28] a definição do porte de uma empresa, baseia-se no número de funcionários e no valor da faturação bruta anual, conforme indicado no Quadro 1 e 2.

PORTE	NÚMERO DE FUNCIONÁRIOS
MicroEmpresa	Até 10
Pequena Empresa	**Mais de 10 e até 100**
Média Empresa	**Mais de 100 e até 200**
Grande Empresa	Acima de 200

Tabela 3 – Classificação de empresas por número de funcionários
Fonte: ANIP, 2012

PORTE	FATURAÇÃO BRUTA ANUAL
MicroEmpresa	Não superior a 250.000 USD
Pequena Empresa	**Superior a 250.000,00 USD e =< 3.000.000,00**
Média Empresa	**Superior a 3.000.000,00 USD e =< 10.000.000,00 USD**
Grande Empresa	Acima dos 10.000.000,00 USD

Tabela 4 – Classificação de empresas por faturação bruta anual
Fonte: ANIP, 2012

[27] Novo regime das Micro, Pequenas e Médias Empresas.
[28] Agência Nacional de Investimento Privado.

CAPÍTULO III - METODOLOGIA

Nesta fase, são descritos os procedimentos metodológicos que servem como guia desta pesquisa. Em sequência, são apresentados a classificação da metodologia quanto aos objectivos e procedimentos técnicos da pesquisa, os objetos e sujeitos da pesquisa, os procedimentos utilizados na recolha de dados e os procedimentos relativos a análise e interpretação dos dados.

3.1 Classificação da Metodologia

3.1.1 Classificação da Pesquisa com Base nos Seus Objetivos

A pesquisa deste trabalho é classificada como exploratória e descritiva. De acordo com Gil (2002) a pesquisa exploratória é fundamental para um trabalho científico, pois proporciona maior informação sobre um tema, tornando-o mais claro. Esse tipo de pesquisa contribui para o aprimoramento de ideias e descoberta de intuições que servem para construção de hipóteses. Ela envolve na maioria dos casos o levantamento bibliográfico e entrevistas com pessoas que têm experiências com o problema pesquisado. Quanto a pesquisa descritiva e ainda, segundo o autor, tem como objectivo descrever as caraterísticas de um determinado fenómeno e estabelecer a relação entre as variações no objeto de estudo analisado.

Em face disto, para este trabalho, a abordagem exploratória visa aprofundar e oferecer maior conhecimento sobre o tema em estudo, dando os *inputs* necessários para a sistematização do trabalho, uma vez existir pouca literatura sobre o tema segurança da informação. Assim, o estudo visa aumentar o conhecimento desta temática e investigar como as PMEs com realce aos do sector bancário de Angola realizam a gestão da segurança da informação. A abordagem descritiva procura descrever as caraterísticas do fenómeno e sua ocorrência em três empresas angolanas, com vista à conhecê-las melhor.

3.1.2 Classificação da Pesquisa Quanto à Sua Natureza

A pesquisa é de natureza qualitativa, atendendo que não são utilizados dados estatísticos no processo de análise do problema em estudo. A abordagem qualitativa é a que se adequa aos objetivos do estudo, porque se pretende entender detalhadamente as variáveis do fenómeno, como é descrito neste trabalho.

3.2 Classificação da Pesquisa com Base nos Procedimentos Técnicos

Segundo Gil (2002, p. 43)

> *"A classificação das pesquisas em exploratórias, descritivas e explicativas é muito útil para o estabelecimento de seu marco teórico, ou seja, para possibilitar uma aproximação conceitual. Todavia, para analisar os fatos do ponto de vista empírico, para confrontar a visão teórica com os dados da realidade, torna-se necessário traçar um modelo conceitual e operativo da pesquisa".*

Ainda de acordo com o autor, o modelo conceitual e operativo da pesquisa recebe o nome de delineamento, que faz referência ao planeamento da pesquisa numa dimensão mais ampla. Um delineamento é identificado através do procedimento adotado para a recolha de dados**.** Neste contexto, quanto ao delineamento da pesquisa em que se definiram os passos utilizados para a sua operacionalização, foi primeiro utilizado a pesquisa bibliográfica por ser o primeiro passo na orientação de um trabalho científico e estudo de caso, tendo este envolvido três organizações angolanas.

O estudo de caso já foi visto como procedimento pouco rigoroso e que fornece pouca base para generalizações. Mas, atualmente, é visto como o delineamento mais adequado para a investigação de um fenómeno atual dentro de seu contexto real, onde os limites entre o fenómeno e o contexto, não são claramente definidos (Yin 2005). Deste modo, convém referir, ainda que, o que se procura é generalizar proposições teóricas e não proposições sobre populações. O estudo de caso pode indicar o grau de generalização de proposições.

Tendo em conta a questão da pesquisa "Como as PMEs realizam gestão da segurança da informação" optou-se por realizar um estudo de caso. Conforme Yin (2005) o estudo de caso constitui uma estratégia de pesquisa utilizada pelos investigadores com bastante regularidade. Dizer que é a estratégia mais utilizada quando se pretende conhecer o "como?" e o "porquê?" certos fenómenos ocorrem, quando o investigador possui pouco controlo dos acontecimentos pesquisados e quando o campo de investigação se concentra num fenómeno natural dentro de um contexto da vida real.

Neste contexto, foi elaborado de acordo com Yin (2005) um projecto para o estudo de caso que contém cinco componentes principais como segue:

- Questões do estudo;
- Proposições;
- Unidades de análise;

- Lógica dos dados;
- Critérios de interpretação e constatação

Os cinco componentes acima ilustrados constituem a estrutura deste estudo de caso, pelo que começarão a ser tratados já a seguir.

Quanto as questões de estudo, de referir que será de acordo ao método apropriado relativamente a estratégia da pesquisa escolhida e já mencionada anteriormente.

No que concerne as proposições é o elemento fundamental na construção de questões que conduzem o estudo de caso na direcção certa. Uma proposição não só reflecte uma questão teórica como também mostra onde procurar as questões relevantes para o estudo (Yin, 2005). Assim, as proposições do estudo refletirão os objetivos específicos desta temática como apresenta o quadro abaixo:

Ojetivo Específico	Proposição
Verificar como as pequenas e médias empresas realizam gestão da segurança da informação.	- O desenvolvimento de uma política de segurança da informação é importante para deixar claro o compromisso da direção para com a segurança da informação, pois é por meio dela que a organização determina o que deve ser considerado como aceitável ou inaceitável. - A implementação de um sistema de gestão de segurança da informação, é uma mais valia, pois estabelece medidas de segurança adequadas que proporciona um grau de importância para o negócio.
Identificar e relatar as atividades e procedimentos adotados para a gestão da segurança da informação.	A implementação de práticas de segurança da informação, não se limita em meios tecnológicos, uma vez que a informação pode existir em vários formatos. Adotar procedimentos de acordo com os padrões internacionais, demonstra preocupação inerente da alta administração da empresa. Isto contribui para a vantagem competitiva.
Demonstrar como as boas práticas de gestão da segurança da informação são um meio necessário para garantir a continuidade do negócio em caso de ocorrência de um incidente;	A aplicação no negócio de medidas de protecção apropriadas contra ameaças que podem causar algum incidente, garante a continuidade do negócio, mesmo que o impacto causado seja alto. Isto exerce influência na vantagem competitiva.

Tabela 5 – Proposições da pesquisa
Fonte: Com base nos dados da pesquisa

A partir do conceito de estudo de caso proposto por Yin (2005), a utilização do método do caso como estratégia para guiar a realização deste trabalho justifica-se pelas seguintes razões:

- A gestão da segurança da informação é um fenómeno novo que ainda não está claramente definida;
- O estudo baseia-se em várias fontes de evidência, tais como: revisão da literatura de teorias de gestão da segurança da informação e entrevistas com gestores de tecnologia de informação de empresas angolanas.

A proposição teórica apresentada com base nos objetivos específicos no capítulo da revisão da literatura orientou a condução e análise do estudo de caso.

De acordo com os conceitos apresentados, a opção pela utilização do método de estudo do caso parece adequada para atingir os objetivos propostos pela pesquisa, que é o de investigar porque as PMEs adotam a gestão da segurança da informação.

3.2.3 Seleção do caso para estudo

Para Creswell (1994) o investigador ao escolher o caso estabelece uma ligação lógica que serve de guia de todo o processo de recolha de dados.

Neste contexto, no projecto de estudo de caso e segundo Yin (2005) pode-se optar por estudar como segue:

- um caso único, de uma única unidade de análise;
- caso único de várias unidades de análise;
- dois ou mais casos com uma unidade de análise para cada caso; e
- dois ou mais casos com várias unidades de análise para cada caso.

Com o exposto acima, e de acordo as características da pesquisa, escolheu-se realizar um estudo de caso que envolveu três empresas. Isto requer uma metodologia mais apurada, por ser necessária a replicação das mesmas questões em todos os casos. Como diz Yin (2005) este tipo de estudo, apresenta evidências mais convincentes e deve seguir uma lógica de replicação (seja ela literal ou teórica) e não de amostragem.

O presente estudo é de natureza exploratória por permitir encontrar os cenários nas organizações alvos do estudo sobre a temática em questão.

3.2.4 Caraterísticas das empresas escolhidas

As empresas escolhidas para o estudo são do ramo financeiro, concretamente do segmento bancário. Optou-se por escolher três bancos, por apresentarem, atendendo ao seu *core business*, matéria relevante para a realização deste estudo.

Os gestores de TI dos respetivos bancos foram os sujeitos da pesquisa. A escolha foi baseada na função pelo fato dos mesmos responderem pelos aspetos relacionados com a tecnologia de informação nas suas organizações e serem conscientes da necessidade de práticas de gestão de segurança da informação.

3.2.5 Protocolo de estudo de caso

A elaboração de um protocolo é importante nas pesquisas de casos múltiplos, pois, constitui, uma das melhores formas de aumentar a confiabilidade do estudo de caso (Gil, 2002). De acordo com Yin (2005) o protocolo contém as regras e procedimentos que devem ser seguidos ao realizar o estudo de caso. Abaixo os principais componentes de um protocolo conforme Yin (2005):

- visão geral do projeto;
- procedimentos de campo;
- questões do estudo; e
- um guia para o relatório do estudo do caso.

Assim, apresentamos a seguir o protocolo de estudo de caso referente a esta pesquisa.

3.2.5.1 Visão geral

No que concerne a visão geral do protocolo desenvolvido, foi feito um pedido formal, entregue às empresas sobre a participação na pesquisa, que dentre outros teores contêm os dados do investigador, objectivo geral, conforme apresentado no Anexo A.

3.2.5.2 Procedimentos de Campo

Esta etapa tem a ver com a parte prática que levou à realização da recolha de dados. Primeiramente foi feito um contacto com as respetivas organizações objetos deste estudo e entrevistados. O contacto foi realizado pessoalmente e autorizado pelos respetivos responsáveis da àrea de TI para realização da pesquisa.

O passo a seguir foi a recolha de dados, realizada através de técnicas e métodos de pesquisa como a entrevista semi-estruturada que foi a principal fonte de evidências de dados utilizada. Deste modo, a recolha de dados, ocorreu por meio de entrevistas que na opinião de Alves (2007), a entrevista é considerada como uma das principais técnicas de recolha de dados pelas vantagens que contempla, uma vez que a interação que se estabelece entre o entrevistador e o entrevistado permite a recolha de informações importantes, bem como aprofundar os dados fornecidos e realizar correções dos mesmos ao ouvir directamente a fonte. Assim, a entrevista é uma das fontes de informação mais importantes e essenciais, nos estudos de caso (Yin, 2005). Neste contexto abordou-se nas entrevistas com os responsáveis pela TI sobre a segurança da informação assim como as ações e decisões tomadas a respeito dos métodos de proteção utilizados na organização.

Ainda, no que concerne, a recolha de dados, foi também utilizada a técnica de observação direta que permitiu investigar os métodos de segurança da informação aplicados nas organizações estudadas e conhecer a sua eficácia. As técnicas utilizadas tiveram como objetivo principal, a recolha de dados sobre a segurança da informação das organizações objeto do estudo, em diversas perspetivas.

3.2.5.3 Questões do Estudo de Caso

Relativamente as questões do estudo de caso, conforme Gil (2002) constituem essencialmente lembranças que auxiliam o investigador a concentrar-se nas informações à serem recolhidas. Assim, as questões do estudo de caso que constituiram o foco da pesquisa, juntamente com os objetivos da investigação, são apresentados abaixo como segue:

Grupo	Objetivo da Investigação	Questões do Estudo	Referências
Perfil do Gestor	Identificação dos Gestores de Tecnologia de Informação.	Idade – Função – experiência.	O autor
Perfil da Empresa	Identificação da Empresa.	Natureza – Segmento – Nº de funcionários.	O autor
Segurança da Informação	Verificar como as pequenas e médias empresas realizam gestão da segurança da informação.	Como as organizações estudadas realizam gestão da segurança da informação.	ISO/IEC 27001 – 2005; Raggad (2010); BS ISO/IEC 27001 – 2005; Beal (2005); Caruso & Sttefen (1999)
	Identificar e relatar as atividades e procedimentos adotados.	Quais as atividades e procedimentos adotados para a gestão da segurança da informação podem garantir a continuidade do negócio.	

	Demonstrar como as boas práticas de gestão da segurança da informação são um meio necessário para garantir a continuidade do negócio em caso de ocorrência de um incidente.	Como as boas práticas de gestão da segurança da informação podem garantir a continuidade do negócio.	

Tabela 6 - Questões do estudo
Fonte: Eaboração com base nos dados da pesquisa

3.2.5.4 Análise e Interpretação dos Dados

Nesta fase é feita a análise dos dados recolhidos que serviram para o desenvolvimento deste trabalho. O estudo de caso desenvolvido teve como objectivo investigar o porquê da importância da gestão da segurança da informação ser adotada pelas pequenas e médias empresas angolanas como ferramenta indispensável na sua estratégia de negócio com foco na política de segurança da informação e gestão de riscos de segurança da informação por proverem directrizes e controlos inerentes à proteção dos ativos de informação e por abrangerem fatores tecnológico, humano, processos, etc.

Este estudo de caso envolveu três empresas angolanas do ramo financeiro, especificamente três bancos. O estudo de caso quanto à sua natureza foi exploratório tendo em conta o objetivo do tema. A abordagem da pesquisa foi qualitativa, realizada através de técnicas e métodos de pesquisa como entrevista semiestruturada, por meio da observação e a análise documental. A pesquisa também foi bibliográfica, pois foram recolhidos dados através de livros, dissertações, artigos de jornal sobre o tema e *sites* com conteúdos relevantes.

O método de recolha de dados pela observação permitiu notar os métodos de segurança utilizados nas organizações objectos do estudo. Alguns documentos, como estatutos da organização, normas de serviços e proposta para a implementação do SGSI, constituíram a análise documental. As entrevistas, semiestruturadas, sobre a segurança da informação, foram feitas com os Diretores da área de TI das organizações estudadas. As entrevistas foram muito importantes, pois permitiram recolher dados sobre as três organizações, embora com foco em política de segurança da informação e gestão de risco de segurança da informação, debruçou-se de um modo geral sobre os diversos pontos que constituem a segurança da informação.

Tendo em conta que o estudo envolveu três organizações, achou-se importante abordar cada uma isoladamente de acordo aos dados que foram recolhidos durante o procedimento de campo através de métodos já referenciados.

CAPÍTULO IV - O ESTUDO DE CASO REALIZADO NAS TRÊS ORGANIZAÇÕES

As três organizações, objetos do estudo, são tomadas em consideração neste capítulo. A pedido das mesmas, não serão revelados, aqui, os seus nomes como proteção da sua identidade, tendo em conta aos dados sensíveis obtidos por meio da entrevista semiestruturada e que podem expor eventuais vulnerabilidades. Assim, foi atribuido um nome facultativo para cada empresa, passando a serem identificadas como Empresa A, Empresa B e Empresa C.

O governo de Angola, tem criado políticas que servem de apoio ao fomento de organizações dos mais variados domínios, constituindo-se de mais valia para a estabilidade sócio-económico do país. Especificamente, para este estudo, virada para o negócio bancário e segundo a Deloitte, este ano houve um crescimento de 16% em relação a 2013. Existem no país 23 bancos.

A seguir, são tratadas, em detalhe, as três empresas objetos do estudo.

4.1 Empresa A

A Empresa A, fundada há mais de 3 anos, é uma organização financeira, designado como banco e que, tem como objetivo apoiar as pequenas e médias empresas, com a disponibilização de crédito, contribuindo para o desenvolvimento de Angola. Também apoiam os seus clientes na vertente de assistência técnica, desde a criação de uma empresa até a elaboração do estudo de viabilidade económico-financeira.

A Empresa A possui alguns balcões de atendimento na cidade de Luanda e fazem uso constante dos sistemas de informação na realização da sua atividade. A área de TI é composta por 8 colaboradores, dos quais 1 tem o cargo de Diretor, 1 chefe de departamento e mais 6 técnicos. Muitos dos serviços relacionadas com o sistema, são terceirizados. O Director é formado em Engenharia Informática e possui 38 anos de idade.

4.1.1 A Gestão da Segurança da Informação na Empresa A

A segurança da informação na Empresa A é vista no âmbito tecnológico, pautada somente em torno da área de TI. Conforme o gestor da área de TI, a sua maior preocupação é

manter em segurança os ativos tecnológicos. Deste modo, constata-se que há uma fraca cultura com relação a segurança da informação no seu todo.

Indagado sobre como é feita a segurança da informação na organização ou que medidas utilizam para protegerem-se das ameaças, o gestor alegou que usam procedimentos como o antivirus e senha para o acesso ao sistema de informação. Acrescenta ainda que têm o firewall como o suporte de proteção da rede interna da organização contra eventuais ataques oriundos de uma rede externa, já que fazem uso constante da internet. O *backup* ou cópias de segurança é outra medida usada para a proteção da informação, pois em caso de perda pode ser recuperada por esta via.

Foi perguntado ao gestor se já ocorreu algum incidente de segurança da informação na Empresa A, e se o impacto tenha provocado a paralisação da atividade, o mesmo disse que nunca aconteceu nada do gênero que pudesse parar com a atividade, mas lembra que num passado recente, houve um colaborador que deixou de fazer parte da Empresa A, mas continuava a aceder ao sistema da organização e a enviar e-mais como se de um funcionário se tratasse, até que foi descoberto por um outro colega. Disse, ainda, que tem acontecido muitas situações, embora não afetar à paragem do negócio, mas que de alguma forma colocam em risco a atividade da Empresa A, como troca de senhas entre os funcionários, etc.

Denota-se que não existe na Empresa A, monitorização no seu sistema e que não há uma comunicação da DRH à área de TI, informando os colaboradores que tenham deixado a Empresa A ou que tenham sido expulsos. Não havendo esta comunicação, dificilmente a área de TI, saberá se o colaborador deixou de ser quadro da empresa.

O entrevistado, abordado se a SI é parte integrante da estratégia da organização, respondeu que "*A área de TI como sendo a que trata da segurança da informação, ainda não faz parte dos planos estratégicos da organização.*

A segurança da informação na Empresa A é somente preocupação da área de TI que tem garantido a segurança dos ativos tecnológicos.

Tratando-se do centro de processamento de dados (CPD), o entrevistado avançou dizendo que têm um local onde estão instalados os servidores que têm a missão de prover os recursos para a operacionalidade da Empresa A, mas constatou-se que a sala não obedece aos requisitos exigidos para um CPD, pois divide com outras atividades. Um CPD deve estar

numa sala fechada e o seu acesso deve ser para aqueles que estão autorizados a acedê-lo. Os servidores encontram em racks, mas sem tampas laterais.

Quando questionado sobre o porquê da adoção da gestão de segurança da informação, o entrevistado, afirmou que no mundo atual, com a dependência cada vez maior dos serviços, às TI, principalmente na atividade bancária que é totalmente indispensável, requer que se tome medidas adequadas para evitar perda de dinheiro.

Procurou-se verificar na organização as práticas de segurança que favorecem uma boa gestão de segurança da informação, conforme o Tabela abaixo:

Práticas de Segurança da Informação	Na Organização
Política de segurança da informação	Não existe
Responsável para concessão, manutenção, revisão e cancelamento das autorizações de acesso à informação.	Não existe
Existe controlo de acesso lógico.	Existe.
Existe controlo de acesso físico.	Existe.
Existe procedimentos para autorização de acesso a informação.	Não existe.
Existe monitorização e controlo das informações nos ambientes lógicos que garantem o acesso apenas as pessoas autorizadas.	Não existe.
As estações de trabalho estão protegidas por uma firewall e um software de antivírus.	Existe.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados ou instalados.	Não existe.
Existe cópias de segurança.	Existe.
Existe CPD (centro de processamento de dados).	Existe.

Tabela 7 – Práticas de Segurança da Informação
Fonte: Com base nos dados da pesquisa

4.1.2 Política de segurança da informação

Quanto a este item, o entrevistado disse que ainda não existe uma política de segurança de informação na organização. Deste modo, constatou-se que as medidas de segurança usados na organização, são feitas de forma empírica, sem estarem definidas num documento que estabelece regras de utilização do sistema de informação para a segurança e controlo do acesso lógico e físico do ambiente na organização.

Mas o entrevistado, acha que a política de segurança da informação quando for implementada na Empresa A, será o porta estandarte, para que a segurança da informação seja considerada como fundamental na estratégia de negócio da organização.

Perguntado sobre a importância que teria a política de segurança da informação, o gestor afirmou "*se tivessemos um documento deste, implementado na organização, teriamos os procedimentos de segurança melhor definidos*".

Reconheceu que as medidas de segurança utilizadas não são suficientemente eficazes para garantir coesão na proteção de seus ativos e que com uma política de segurança da informação, que engloba todos os aspetos relevantes da segurança da informação com conceitos, regras ou diretrizes, que estabeleça responsabilidades e penalizações, ajuda na sensibilização dos funcionários quanto ao valor da segurança da informação assim como mitigar eventuais incidentes de segurança que ponham em risco a atividade da Empresa A.

4.1.2.2 Gestão de Risco de Segurança da Informação

A gestão de risco ainda não é prática na Empresa A, isto é, ainda não existe um processo formal definido, mas de um modo geral, preocupam-se com os riscos a que estão expostos os seus ativos. Segundo o interlocutor, utilizam apenas medidas atenuativas para minorar os riscos que na maioria das vezes acontecem de forma desregrada por não ser um processo cíclico.

Perguntado porque acha necessário proteger os ativos de informação da Empresa A, o entrevistado respondeu que existem ameaças e riscos que se não forem tomadas as devidas precauções pode ocorrer um incidente com impacto devastador como a paragem do negócio. Convidado a definir ativo, definiu da seguinte forma: "*Ativo são os equipamentos que servem de suporte ao negócio*"

O gestor tem consciência de que qualquer organização que faça uso de tecnologia de informação, está sujeita a correr riscos por causa das ameaças que estão sempre as espreitas.

Abordado sobre ameaças que são a fonte de um incidente e quais os procedimentos adotados para evitar que explorem vulnerabilidades dos ativos da organização, o entrevistado afirmou que usam medidas de deteção que, na sua visão, ajudam a reduzir as vulnerabilidades

e impedir que ocorra um incidente. Como medidas de deteção utilizam detetores de intrusão, câmeras de vigilância, dentre outras.

Quando indagado sobre o que compõe um processo de gestão de risco, o gestor da organização A, é de opinião que os riscos devem ser tratados de acordo com uma lógica que se debruce sobre a questão das ameaças.

Foi constatado que não existindo na organização uma política de segurança definida, aos riscos identificados não são dados o tratamento devido, isto é, o seu tratamento não é de acordo a sua caraterística, são tratados de forma reativa e ainda assim, consideram que mantém preservados os seus ativos.

A informação na Empresa A, ainda não é classificada. É importante a organização ter definida quais informações devem ser consideradas críticas para se definir o seu valor e como proteger das ameaças e risco de segurança da informação.

Procurou-se verificar na organização as práticas de segurança que favorecem uma boa gestão de segurança da informação, conforme o quadro abaixo:

Práticas de Gestão de Risco de Segurança da Informação	**Na Organização**
Existe plano de identificação, análise/avaliação e tratamento de risco.	Não existe
Todos computadores ligados a rede da organização estão protegidos contra ameaças à rede via firewall.	existe.
Antivírus configurado para protecção e funcionamento em tempo real.	existe.
Existe um local remoto para armazenar as cópias de segurança.	Não existe.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados ou instalados.	Não existe.
Alerta caso mais de 10% da rede estiver com as definições de vírus desactualizada.	Não existe.
Lista de técnicos credenciados autorizados a entrar no CPD.	Não existe.
Existe plano de contigência para a continuidade de negócio.	Não existe.
A informação da organização é classificada em informação pública, interna geral, interna restrita e confidencial.	Não existe

Tabela 8 – Práticas de Gestão de Risco de Segurança da Informação
Fonte: Elaborada com base nos dados da pesquisa

4.2 EMPRESA B

A Empresa B, está no mercado a mais de 5 anos e semelhante a Empresa A, o seu ramo de actividade é o sector bancário e, está situada em Luanda. Possui uma carteira de clientes aceitável e o seu objetivo é oferecer produtos e serviços financeiros competitivos que contribuam para o desenvolvimento de Angola.

A área de Tecnologia de Informação é chefiada por um profissional de 39 anos de idade, que tem a função de gerí-la, conjuntamente com mais 9 colaboradores, sendo que 1 chefe de Departamento e 8 técnicos, constituindo a equipa de TI. Também é licenciado em Engenharia Informática.

4.2.1 A Gestão da Segurança da Informação na Empresa B

Para o Diretor de TI da Empresa B a segurança da informação é muito importante, sendo o negócio um banco, procuram manter operacional em tempo real os seus equipamentos por servirem de suporte ao negócio. Segundo o gestor:

> *Temos constituído controlo de acesso lógico e físico, realizados através de mecanismos e procedimentos que resultam na protecção do sistema de informação e do ambiente da organização contra acessos não autorizados.*

Quando perguntado se já ocorreu algum incidente de segurança da informação na Empresa B, e se o impacto tenha provocado a paralisação da atividade, o gestor foi peremptório ao afirmar que nunca desde que ele está na Empresa B, aconteceu um incidente que causasse interrupção dos serviços. Constatou-se que não existe um processo de monitorização do seu sistema para identificar eventuais violações, como acesso à rede por pessoas não autorizadas.

Questionado quanto as medidas de segurança da informação aplicadas, respondeu que recorrem a prática do uso de autenticação dos utilizadores como senha de acesso, antivírus e *firewall*.

Abordado sobre o CPD da Empresa B, constatou-se que possui janela para o exterior, revelando deste modo uma vulnerabilidade, pois pode ser facilmente alvo de um ataque. O sistema de ventilação ou ar condicionado não funciona com regularidade e não possui energia redundante, podendo deste modo, causar um mau funcionamento dos equipamentos. Outra situação incorreta verificada são os racks que suportam os servidores, switches, os roteadores

encontrados em estado de abertos e cheios de pó, estando em situação de inconformidade de acordo com os padrões definidos internacionalmente.

Indagado sobre se a administração de topo vê a segurança da informação, como elemento estratégico dos seus planos de negócio, o gestor respondeu como segue:

> *Como estratégia em si, ainda não, mas existe interesse da parte da administração em dar maior engajamento ao processo de segurança da informação, separando a segurança da informação da área de TI, com objetivo de melhor coordenar a SI e assim, garantir que os sistemas de informação da organização, são adequadamente protegidos.*

Mas, o entrevistado não entende que a segurança da informação para além dos ativos tecnológicos depende também de fatores humanos, de processos, etc. E Convidado a falar sobre a implementação de um SGSI, foi categórico ao dizer que:

> *Quando a SI se tornar independente da área de TI, haverá maior preocupação, com o enquadramento da segurança da informação na nossa instituição e desta forma, a gestão da segurança da informação terá maior visibilidade dentro da organização. E com o envolvimento da administração de topo neste processo, acredito que a segurança da informação, fará parte do plano estratégico da organização.*

O interlocutor, alegou, quando questionado sobre o porquê da adoção da gestão de segurança da informação, que serve para proteger o negócio contra perda financeira e roubo de informação sensível, que poria em causa a imagem da Empresa B, perante o mercado e seus clientes.

Procurou-se verificar na organização as práticas de segurança que favorecem uma boa gestão de segurança da informação, conforme o quadro abaixo:

Práticas de Segurança da Informação	**Na Organização**
Política de segurança da informação	Não existe
Responsável para concessão, manutenção, revisão e cancelamento das autorizações de acesso à informação.	Não existe
Existe controlo de acesso lógico.	Existe.
Existe controlo de acesso físico.	Existe.
Existe procedimentos para autorização de acesso a informação.	Não existe.
Existe monitorização e controlo das informações nos ambientes lógicos que garantem o acesso apenas as pessoas autorizadas.	Não existe.
As estações de trabalho estão protegidas por uma firewall e um software de antivírus.	Existe.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados	Não existe.

ou instalados.	
Existe cópias de segurança.	Existe.
Existe CPD (centro de processamento de dados).	Existe.

Tabela 9 – Práticas de Segurança da Informação
Fonte: Com Base nos dados da Pesquisa

4.2.2 Política de Segurança da Informação

Quanto a política de segurança da informação, o gestor alegou que ainda não existe, mas garantiu que já foram alertados pelo BNA (Banco Nacional de Angola), quanto a esta questão. Para o gestor, a política, quando for implementada servirá de alavanca para o asseguramento dos seus ativos da informação.

Quanto a importância da política de segurança da informação, o mesmo afirmou o seguinte: "*A política de segurança da informação ajuda a preservar os recursos do Banco, impondo regras e procedimentos para a sua utilização, possibilitando deste modo que se tenha um controlo sobre os riscos.*

O gestor, não foi capaz de dizer em que contexto será elaborada a política. Uma política de segurança da informação, conforme a ISO 27001, é elaborada de acordo a necessidade de segurança de uma organização e deve ser aplicada à todos os funcionários, as empresas que prestam serviços ou terceiros que utilizam o ambiente do sistema de informação da organização ou que tenham acesso as informações da mesma.

4.2.3 Gestão de Risco de Segurança da Informação

A gestão de risco, ainda não é realizada na Empresa B, mas procuram proceder de acordo com as práticas que permitem controlar os riscos.

Perguntado sobre a necessidade de proteger os ativos de informação contra os riscos existentes, o gestor alega que protegem os ativos de informação para evitar que incidentes ocorram e não haja paragem na atividade e fornecimento de serviços, pois que, com o impacto, seria prejudicial para o negócio. Ativo, para o entrevistado, é "*Qualquer componente como seja, tecnológico que sustenta um ou mais processos de negócio da organização*".

Na Empresa B, não ocorre nenhum processo de identificação de ameaças que podem colocar em causa a continuidade de negócio da organização e perguntado sobre ameaças que são a fonte de incidentes e quais são os procedimentos adotados na organização, para evitar que ameaças explorem vulnerabilidades dos seus ativos, o interlocutor afirmou que a instituição possui mecanismos de controlo, para acesso ao ambiente físico e lógico da Empresa B.

Deste modo, segundo o interlocutor, o colaborador à entrada das instalações, deve exibir um cartão de acesso e para o acesso as aplicações da Empresa B, o uso de senha. Sustentou ainda que têm instalado nos seus sistemas, firewall, antivírus e que contará também no futuro com a política de segurança da informação.

Indagado sobre o que compõe um processo de gestão de risco, o gestor da Empresa B, demonstrou conhecer o seu ciclo, ao ilustrar os passos subsequentes, afirmando que, "a gestão de risco, inicia com o processo de identificação, avaliação, para se medir o nível de risco e serem, então, definidas para tratamento, as medidas apropriadas para a sua mitigação.

Quanto a classificação da informação, ainda é inexistente na Empresa B, mas segundo o seu gestor de TI, quando for implementado o sistema de gestão de segurança da informação, terão as suas informações classificadas de acordo ao seu grau de importância.

Procurou-se verificar na organização as práticas de segurança que favorecem uma boa gestão de segurança da informação, conforme a tabela abaixo:

Práticas de Gestão de Risco de Segurança da Informação	**Na Organização**
Existe plano de identificação, análise/avaliação e tratamento do risco.	Não existe.
Todos computadores ligados a rede da organização estão protegidos contra ameaças à rede via firewall.	Existe.
Antivírus configurado para protecção e funcionamento em tempo real.	Existe.
Existe um local remoto para armazenar as cópias de segurança.	Não existe.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados ou instalados.	Não existe.
Alerta caso mais de 10% da rede estiver com as definições de vírus desactualizada.	Não existe.

Lista de técnicos credenciados autorizados a entrar no CPD.	Não existe.
Existe plano de contigência para a continuidade de negócio.	Não existe.
A informação da organização é classificada em informação pública, interna geral, interna restrita e confidencial..	Não existe

Tabela 10 – Práticas de Gestão de Risco de Segurança da Informação
Fonte: Elaborada com base nos dados da pesquisa

4.3 EMPRESA C

Este caso, refere-se a uma empresa que tem a sua sede em Luanda (Angola) e exerce a sua atividade bancária há mais de 8 anos. O seu objetivo é procurar ser um parceiro bancário de referência e fornecer serviços financeiros capazes de responder positivamente as necessidades dos seus clientes.

A Empresa C tem como gestor de Segurança da Informação, um profissional com formação em Engenharia Informática e, pós-graduação em gestão da segurança da informação, de 48 anos de idade. O gestor faz parte de um gabinete subdividido em duas áreas a saber: segurança informática e segurança eletrónica, tratando-se uma de aspetos relacionados com a TI e outro com a questão dos acessos, câmeras de vigilância, etc. De acordo com o estatuto da Empresa C, o gabinete é um órgão de *staff* da alta administração, criado para dar suporte ao negócio da empresa, concernente a segurança informática e eletrónica, constituindo-se de fundamental na supervisão à área de Tecnologia de Informação). Importa realçar, que neste caso em concreto, há um segundo entrevistado que é o gestor de TI, profissional formado em Engenharia Informática, de 40 anos de idade. O quadro de pessoal da área de TI é composto por 15 elementos, sendo 1 Diretor, 1 chefe de Departamento e 13 técnicos. A área nova tem apenas 5 colaboradores, dos quais 1 designado Diretor, 1 Analista de SI e três tecnicos de SE (segurança eletrónica).

4.3.1 A Gestão da Segurança da Informação Na Empresa C

Relativamente sobre este ponto (gestão da segurança da informação), o entrevistado da Empresa C, no caso, o gestor do GSI (gabinete de segrança integrada), alegou que o seu gabinete tem a incumbência de fazer a gestão da segurança da informação na Empresa C e o seu objetivo é a criação de políticas e processos de segurança da informação, com vista a

aplicação de medidas de controlo, para manter a salvaguarda do negócio da Empresa C, em caso de ter de enfrentar situações anómalas que ponham em risco o negócio da instituição.

Foi perguntado ao gestor de TI se já ocorreu algum incidente de segurança da informação na Empresa C, e se o impacto tenha provocado a paralisação da atividade. O responsável de TI da Empresa C, respondeu o seguinte:

> *Vou citar apenas um caso, dentre os vários que já aconteceram, ou seja, há um tempo atrás o funcionário indicado para neste dia efetuar o fecho, fez uma operação inadvertida que originou a não realização do fecho na altura devida, causando deste modo falta de sistema durante o dia todo, com impacto relevante, pois os clientes não poderam efetuar as sua transações normais, como depósitos, transferências, levantamento de valores, entre outras operações.*

Quando indagado sobre quais medidas de segurança da informação está implementada na Empresa C, o gestor do GSI disse o seguinte:

> *Somos nós que emitimos os passes de acesso, fazemos a gestão das câmeras de vigilância, os detectores de intrusão e as políticas de segurança da informação de acordo com a ISO 27001. Procuramos garantir que as práticas de segurança da informação, são observadas ou estão em conformidade com as directrizes definidas na política, garantindo a confidencialidade, integridade e disponibilidade da informação.*

Para o gestor da DTI, quando perguntado sobre as medidas de segurança da informação aplicada na Empresa C, respondeu que, à proteção do sistema, usam ferramentas como autenticação de utilizadores, *logs*, antívirus e firewall, bem como um aplicativo específico de monitorização, como o *whatsapp* que permite monitorizar a rede ou identificar se há algum balcão em inatividade. Também fazem uso da ferramenta PRTG que serve segundo o gestor, para monitorizar todos os servidores.

Foi constatado que está em curso a implementação do sistema de gestão da segurança da informação.

Quando questionado sobre o CPD, o entrevistado, afirmou que para além do CPD principal, têm um alternativo em outro local como recuperação de desastre. Constatou-se que o centro de processamento de dados da Empresa C é totalmente fechado, possui 2 aparelhos de ar condicionado, mas apenas um fica em funcionamento, ficando outro em estado de retorno em caso de avaria. Verificou-se que os computadores se encontram em bastidores (*racks*) completamente fechados.

O entrevistado, do GSI, quando perguntado se a SI é parte integrante da estratégia de negócio da organização, alegou o seguinte:

> *Sim, até porque esta atividade é recente e conta com o apoio total da administração executiva que, por sinal, foi o grande impulsionador da existência de um setor independente à TI, para olhar especificamente na questão da gestão da segurança da Informação, refletindo, deste modo, a importância da SI nas decisões estratégicas do Banco.*

O entrevistado, quando questionado sobre o porquê da adoção da gestão de segurança da informação, respondeu que é para manter inviolável as suas informações de negócio, sobretudo para evitar a interrupção das atividades do Banco, pois isso representaria risco de perda financeira, degradação da imagem no mercado e insatisfação do seu maior património que são os seus clientes.

Procurou-se verificar na organização as práticas de segurança que favorecem uma boa gestão de segurança da informação, conforme o quadro abaixo:

Práticas de Segurança da Informação	Na Empresa
Política de segurança da informação	Existe
Responsável para concessão, manutenção, revisão e cancelamento das autorizações de acesso à informação.	Não existe
Existe controlo de acesso lógico.	Existe.
Existe controlo de acesso físico.	Existe.
Existe procedimentos para autorização de acesso a informação.	Existe.
Existe monitorização e controlo das informações nos ambientes lógicos que garantem o acesso apenas as pessoas autorizadas.	Existe.
As estações de trabalho estão protegidas por uma firewall e um software de antivírus.	Existe.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados ou instalados.	Existe.
Existe cópias de segurança.	Existe.
Existe CPD (centro de processamento de dados).	Existe.

Tabela 11 – Práticas de Segurança da Informação
Fonte: Com Base nos dados da Pesquisa

4.3.2 Política de segurança da informação

Sobre esta temática, já é prática na Empresa C, pois foi recentemente elaborada uma política global de segurança da informação e várias outras políticas com base na ISO 27001. O gestor do GSI alegou que já têm definido planos de atuação para realizar os controlos, uma vez que as políticas já foram definidas.

A definição das políticas de Segurança da Informação na Empresa C foram elaboradas pelo GSI em parceria com uma consultora externa. À sua elaboração, envolveu a colaboração de todas unidades que compõe a estrutura da Empresa C, uma vez tratar-se de um processo transversal.

Perguntado sobre a importância que tem a política de segurança da informação, o gestor afirmou que: "*A política de segurança da informação, contribui para a proteção da informação, provendo regras para a materialização de métodos para controlar as ameaças e e diminuir os riscos inerentes, garantindo deste modo a disponibilidade, a integridade, a confidencialidade da informação para realização do negócio do Banco*".

4.3.3 Gestão de Risco de Segurança da Informação

A gestão de risco de segurança da informação na Empresa C, já começa a dar os seus primeiros passos, uma vez que já existe uma política global de segurança da infomação e outra definida especificamente para olhar sobre a gestão de risco de segurança da informação.

Ainda não ocorre o processo de gestão de risco de segurança da informação, mas já possuem um plano elaborado com vista a classificar os ativos críticos para serem identificados provavéis riscos e assim serem medidos de acordo seu valor para então serem definidas medidas de mitigação.

Perguntado sobre quais são os procedimentos adotados na organização, para evitar que ameaças explorem vulnerabilidades dos seus ativos, o gestor de TI, afirmou que os mecanismos instalados nos seus sistemas são medidas de mitigação, como é o caso da configuração de permissões, instalação de softwares anti-vírus, *firewall*, dentre outros. A aplicação dessas medidas na Empresa C, já é feita com base nas políticas recentemente criadas e não de forma intuitiva como era prática.

O gestor do GSI, perguntado se existe algum tipo de classificação da informação na Empresa C, respondeu que sim, e que encontram-se classificadas da seguinte forma:

- informação pública; interna geral; interna restrita; e confidencial.

Perguntado porque acha necessário proteger os ativos de informação da Empresa C, o interlocutor do GSI respondeu ser pelo fato de se encontrarem sempre expostos a ameaças e para não se perderem informações cruciais ao negócio da Empresa C, implantam medidas de

controlo para evitar que elas (ameaças) provoquem incidente que pode de algum modo causar impacto no funcionamento normal das atividades com a perda de integridade e disponibilidade dos dados.

Ativo, para o gestor "*é tudo que tem valor para o nosso Banco. Não trata-se apenas dos recursos tecnológicos, mas também dos processos e pessoas que estão envolvidas na funcionalidade do Banco*.

Procurou-se verificar na organização as práticas de segurança que favorecem uma boa gestão de segurança da informação, conforme o quadro abaixo:

Práticas de Gestão de Risco de Segurança da Informação	**Na Empresa C**
Existe plano de identificação, análise/avaliação e de tratamento de risco.	Existe, faltando apenas a sua execução.
Todos computadores ligados a rede corporativa estão protegidos contra ameaças à rede via firewall.	Existe.
Antivírus configurado para protecção e funcionamento em tempo real.	Existe.
Existe um local remoto para armazenar as cópias de segurança.	Existe.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados ou instalados.	Não existe.
Alerta caso mais de 10% da rede estiver com as definições de vírus desactualizada.	Não existe.
Lista de técnicos credenciados autorizados a entrar no CPD.	Não existe.
Existe plano de contigência para a continuidade de negócio.	Não existe.
Existe classificação da informação na organização.	Existe

Tabela 12 – Práticas de Gestão de Risco de Segurança da Informação
Fonte: Elaborada com base nos dados da pesquisa

CAPÍTULO V - ANÁLISE E DISCUSSÃO DOS RESULTADOS

Após a apresentação da descrição dos casos que reflectem a pesquisa, começa-se neste capítulo uma abordagem relativa à análise comparativa dos casos, fazendo análise das principais semelhanças e diferenças verificadas na revisão da literatura conforme pensamento dos autores apresentados.

5.1 Análise Comparativa do Perfil dos gestores e de suas organizações

Todos os interlocutores têm formação superior em engenharia informática, com realce à um, por possuír especialização em gestão da segurança da informação. A tabela abaixo, apresenta, os dados relativos as caraterísticas dos sujeitos e objetos da pesquisa.

	Organização A	**Organização B**	**Organização C**	
Idade do gestor	38 anos	39 anos	48 anos	40anos
Gênero	Masculino	Masculino	Masculino	
Formação académica	Engenharia Informática	Engenharia Informática	Engenharia Informática	
Pós-graduação	Não possui	Não possui	Gestão da Segurança da Informação	Não possui
Cargo atual na organização	Diretor de TI	Diretor de TI	Diretor de GSI[29]	Diretor de TI
Tempo no cargo	4 Anos	2 Anos	1 Ano	3 Ano

Tabela 13 – Apresentação comparativa dos gestores entrevistados.
Fonte: Elaboração com base nos dados da pesquisa

Os gestores são colaboradores de empresas privadas. Em termos de experiência, verificou-se que o gestor da Empresa A possui maior quantidade de anos e o único que tem formação em pós-graduação é o gestor da Empresa C. Ele é o que tem maior conhecimento sobre gestão da segurança da informação, atendendo a sua formação.

Relativamente às organizações estudadas, tratou-se de empresas do setor privado, denotando-se diferenças, quer no número de funcionários, caraterísticas da infraestrutura de TI, como também em termos de práticas de gestão de segurança da informação empregadas em cada uma delas. Desse modo, achou-se imperioso realizar o estudo sobre organizações com perfis diferentes no que toca à gestão da segurança da informação.

[29] Gabinete de Segurança Integrada

	Empresa A	**Empresa B**	**Empresa C**
Existência (anos)	Mais de 3	Mais de 5	Mais de 8
Número de colaboradores	75	102	155
Número de colaboradores de TI e SI[30]	8	10	20
Número de estações de trabalho	69	95	147

Tabela 14 – Comparação das caraterísticas das organizações objecto da pesquisa
Fonte: Com base na pesquisa

5.2 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Pode-se perceber através do gestor da Empresa A, que a segurança da informação está virada para o aspeto tecnológico, e que são usadas medidas para proteção da informação, o antivirus, senha de acesso, *firewall* e também cópias de segurança deduzindo-se deste modo, que a visão sobre SI é míope. De igual modo, a Empresa B recorre as mesmas medidas praticada pela Empresa A.

O gestor da Empresa C, mostrou que tem conhecimento sobre gestão da segurança da informação uma vez que o seu gabinete é responsável pela elaboração de políticas de segurança da informação assim como os processos de segurança da informação. Procuram garantir que a confidencialidade, integridade e a disponibilidade estejam asseguradas.

Apenas o gestor da Empresa C foi capaz de usar os termos de referência dos princípios de segurança da informação que são a confidencialidade, integridade e a disponibilidade, quando perguntado sobre quais medidas de segurança estão implementados na Empresa C. Este conhecimento está de acordo com os autores Beal (2005), Gelbstein e Kamal (2002), Sêmola (2003), que afirmam que o objetivo da segurança da informação é a preservação dos três pilares que são a confidencialidade, integridade e disponibilidade.

Relativamente às medidas de segurança, qualquer uma das empresas, recorre as ferramentas antivírus, uso de senha, firewall como forma de mitigar as ameaças a que estão expostas.

[30] Refere exclusivamente à Empresa C.

A segurança da informação, para as empresas A e B, ainda não são consideradas como fundamentais na estratégia de negócio, sendo apenas a Empresa C que tem o apoio da administração de topo e é vista como parte integrante da estratégia do seu negócio.

Todos os interlocutores foram unânimes quanto à adopção da gestão da segurança da informação ao afirmarem que o objetivo é evitar perda financeira.

Podemos verificar na tabela abaixo, alguma discrepância relativamente às práticas de segurança da informação entre as três empresas:

Práticas de Segurança da Informação	Empresa A	Empresa B	Empresa C
Política de segurança da informação	Não existe	Não existe	Existe
Responsável para concessão, manutenção, revisão e cancelamento das autorizações de acesso à informação.	Não existe	Não existe	Não existe
Existe controlo de acesso lógico.	Existe.	Existe.	Existe.
Existe controlo de acesso físico.	Existe.	Existe.	Existe.
Existe procedimentos para autorização de acesso a informação.	Não existe.	Não existe.	Não existe.
Existe monitorização e controlo das informações nos ambientes lógicos que garantem o acesso apenas as pessoas autorizadas.	Não existe.	Não existe.	Existe.
As estações de trabalho estão protegidas por uma firewall e um software de antivírus.	Existe.	Existe.	Existe.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados ou instalados.	Não existe.	Não existe.	Não existe.
Existe cópias de segurança.	Existe.	Existe.	Existe.
Existe CPD (centro de processamento de dados).	Existe.	Existe.	Existe.

Tabela 15 – Comparação das Práticas de Segurança da Informação das organizações pesquisadas
Fonte: Com base na pesquisa

Fazendo menção aos dados apresentados na tabela, concluimos que a segurança da informação nas três empresas ainda é débil, embora terem como prática algumas medidas que podem de alguma forma mitigar os riscos inerentes. Podemos notar que a Empresa C, tem uma visão diferente das outras, pois já tem constituida uma política de segurança da informação. É importante que estas empresas tenham uma visão daquilo que são definidos pelos vários autores sobre a temática segurança da informação, para melhor protegerem os seus ativos, de modo a atingir os objetivos estratégicos definidos.

Todas as empresas estudadas possuem CPD, mas apenas a Empresa C tem o CPD minimamente em conformidade, pois as outras duas apresentam situações de risco, denotando-se que os equipamentos em *racks* não se encontravam devidamente protegidos.

5.3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Uma política de segurança da informação, constitui uma pedra basilar na proteção da informação de qualquer empresa, pois contém as regras fundamentais que deverão ser implementadas na organização para manter inviolável o negócio. Este é um domínio que deve ser encontrado numa organização que tenha preocupação em implementar práticas de segurança da informação.

No entanto, ainda não se verifica esta prática em duas das três Empresas, de acordo com os resultados apresentados na tabela anterior, mostrarando a inexistência de política de segurança da informação na Empresa A, como também na Empresa B. O entrevistado da Empresa A tem consciência de que quando for elaborada a política de segurança da informação será fundamental na estratégia do negócio. Do mesmo modo, para a Empresa B, a política servirá de alavanca para o asseguramento dos seus ativos da informação.

Em situação diferente, está a Empresa C que já possui uma política de segurança, elaborada de acordo com o padrão internacional ISO 27001. Inclusive, já têm constituido, plano para realização de controlos de monitorização.

Todos os interlocutores foram unânimes quanto a importância da política de segurança da informação, embora com abordagens distintas, mas visando à proteção dos seus ativos. No entanto, apenas o gestor da Empresa C, foi capaz de indicar os três pilares fundamentais da segurança da informação, a confidencialidade, integridade e a disponibilidade conforme retratado na revisão da literatura deste trabalho.

5.4 GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO

Gerir os riscos é um dos principais processos da gestão da segurança da informação que qualquer empresa deveria se procupar, pois visa a identificação, avaliação e priorização de riscos. Este processo é seguido, depois, pela aplicação coordenada e económica dos recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, reduzindo o risco a um nível aceitável.

A Empresa A, não obstante preocupar-se com os riscos existentes, não possui se quer um processo de gestão de risco. Usam algumas medidas de segurança, sem no entanto seguir uma

regra pré-estabelecida. De modo semelhante está a Empresa B, que também não realiza a gestão de risco e pensam que as práticas que utilizam permitem controlar os riscos.

Ao contrário da Empresa A e B, a Empresa C, embora ainda não ocorrer o processo de gestão de risco, possui um plano que visa classificar os ativos críticos, para se ter conhecimento de quais ativos de informação são prioritários na implementação de medidas de mitigação dos riscos.

Os entrevistados têm consciência da necessidade de se proteger os ativos de informação, uma vez que cada um sabe da existência de ameaças que podem colocar em risco a atividade do negócio de suas empresas. Por esta razão consideram importante a tomada de precauções para evitar que incidentes ocorram.

Qualquer uma das três empresas, faz uso de antivírus, firewall e de mecanismo de acesso ao ambiente lógico e físico da organização, mas estas medidas são insuficientes, considerando os vários tipos de ameaças que podem pôr em risco a atividade da organização.

Mas não existindo um processo de gestão de risco, o risco que eventualmente é identificado, não é avaliado de acordo com os parâmetros apropriados que permitem olhar para o valor do ativo e assim conhecer o seu impacto. Portanto sem este processo, acaba-se por aceitar o risco sem ter noção da sua carateristica, tornando inadequado o processo de mitigação.

O cenário das Empresas A e B pode ser considerada de muito preocupante, tendo em conta o seu *core business*, pois a segurança da informação está voltada mais para o âmbito tecnológico e como foi retratado na revisão da literatura, a segurança da informação não se resume somente neste aspeto, considerando também os processos e pessoas.

O gestor da empresa C foi o único que quando perguntado sobre o que entende por ativo conseguiu definir de forma concisa, focando os três aspetos, tecnológico, humano e processos, enquanto que os outros dois gestores consideraram apenas o aspeto tecnológico. Conhecendo-se exatamente o significado de ativo, facilmente se percebe a importância que tem para uma organização, como por exemplo uma informação em papel ou um funcionário são ambos ativos.

Pela característica de seu negócio, a Empresa A e a Empresa B, deveriam preocupar-se mais com a segurança da sua informação, pois é preocupante a não existência de um local remoto para armazenamento das cópias de segurança. Somente a Empresa C, possui um local distante onde preservam as cópias de segurança como recurso para recuperação se acontecer algum incidente.

Outro ponto preocupante e fundamental é o fato de nenhum dos gestores da Empresa A e B ter feito referência aos três princípios básicos da segurança da informação. Desconhecendo esses princípios, dificilmente se consegue ter uma visão de gestão de acordo com o que foi abordado na revisão da literatura. A gestão de risco é feita baseando-se na necessidade de manter assegurado os princípios da segurança da informação contra qualquer violação que ponha em causa a sua perda.

Na Empresa C, ocorre o processo de classificação da informação, constituindo deste modo uma mais valia, por ser um metódo eficaz para a proteção da informação, dotando a organização de conhecimento sobre que informação deve proteger e como proteger. Ao passo que nas outras duas Empresas a informação não é classificada, podendo de algum modo uma informação crítica ser passada para fora da Empresa e captada pela concorrência, por desconhecimento do seu valor.

Pode-se considerar que, de um modo geral, as três empresas estudadas têm implementado poucas medidas de segurança da informação.

Práticas de Gestão de Risco de Segurança da Informação	**Empresa A**	**Empresa B**	**Empresa C**
Existe plano de identificação, análise/avaliação e tratamento do risco.	Não existe	Não existe.	Não existe.
Todos computadores ligados a rede da organização estão protegidos contra ameaças à rede via firewall.	existe.	Existe.	Existe.
Antivírus configurado para protecção e funcionamento em tempo real.	Existe.	Existe.	Existe.
Existe um local remoto para armazenar as cópias de segurança.	Não existe.	Não existe.	Existe.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados ou instalados.	Não existe.	Não existe.	Não existe.
Alerta caso mais de 10% da rede estiver com as definições de vírus desactualizada.	Não existe.	Não existe.	Não existe.
Lista de técnicos credenciados autorizados a entrar no CPD.	Não existe.	Não existe.	Não existe.

Existe plano de contigência para a continuidade de negócio.	Não existe.	Não existe.	Não existe.
A informação da organização é classificada em informação pública, interna geral, interna restrita e confidencial.	Não existe	Não existe	Existe

Tabela 16 – Comparação das Práticas de Gestão de Risco das organizações pesquisadas
Fonte: Com base na pesquisa

Podemos observar na tabela acima, que existe algum equilíbrio entre as três Empresas relativamente quanto ao uso de firewall e antivírus, como medidas de proteção da informação existentes em cada uma delas, mas no geral, somente a Empresa C comparativamente às duas tem vantagem.

Como um centro de processamento de dados é um local crítico, por estarem instalados nele equipamentos sensíveis que suportam as informações de negócio, a sua proteção deve ser seguida com rígor, pois o acesso não deve ser feito por qualquer pessoa, senão aquela que esteja devidamente autorizada. É conveniente que o acesso a ele, seja feito mediante apresentação de um documento que ateste que a pessoa está realmente autorizada a entrar no CPD, assim como deve existir uma lista de pessoas credenciadas ou autorizadas a acedê-lo. Isto permite detectar acessos efetuados irregularmente. Estes procedimentos não são praticados por nenhuma das três empresas estudada.

É de suma importância que as organizações estudadas insiram no seu seio uma cultura de segurança da informação, pois as medidas de proteção ou os controlos existentes nelas, para serem robustos, precisam de uma ação maior ou seja do envolvimento efetivo de todos os seus colaboradores. E uma política de segurança da informação estabelece todo o contexto da segurança da informação, como a nessessidade da prática de gestão do risco da segurança da informação que deve ser executada proativamente, através de procedimentos específicos de forma a acautelar-se dos incidentes.

CAPÍTULO VI - CONCLUSÃO

As empresas estão cada vez mais dependentes da Tecnologia de Informação e, está comprovado no mundo atual que, sem esta ferramenta, as empresas teriam muitas dificuldades na operacionalização dos seus processos. Mas esta dependência deu origem a riscos que precisam ser monitorizados de formas a evitar que acontençam danos ou falhas no fornecimento dos serviços que possam afetar à continuidade do negócio. Neste contexto, o estudo visou investigar por quê das empresas adoptarem a gestão da segurança da informação e como elas gerem para protegerem os seus negócios.

Portanto, foi realizado um estudo de caso em três organizações privadas, do ramo financeiro, localizadas na Província de Luanda.

Observou-se no estudo que a gestão da segurança da informação nestas organizações está mais centrada no âmbito tecnológico. Pode-se observar através das ferramentas de proteção, utilizada por qualquer uma das empresas pesquisadas como é o caso do antivírus, a password e *firewall*, pese embora uma delas, já, seguir o que provê a norma ISO 27001.

A falta de conhecimento sobre os pilares da segurança da informação demonstrado por alguns interlocutores, foi notória. A preocupação pela segurança da informação que se reflete na proteção dos ativos de informação tem como principal objetivo, manter assegurada a confidencialidade, a integridade e a disponibilidade da informação.

Foi verificada, inexistência de práticas relevantes de segurança da informação que não são aplicadas por desconhecimento, levando a que seja imperioso as empresas cultivarem-se mais sobre esta temática.

À questão da política de segurança da informação, pode-se constatar que ainda não é prática em algumas empresas. A falta de política de segurança da informação, representa um grande buraco naquilo que são as práticas de segurança da informação, descritas pelos diversos autores referenciados na revisão da literatura, pois que uma política é um recurso crítico da segurança da informação, por constarem nela todas as considerações fundamentais relacionadas à segurança da informação.

No que toca a gestão de risco, observou-se que as empresas pesquisadas não possuem um processo formal sobre gestão de risco, não obstante mostrarem-se conscientes da necessidade deste processo para um melhor controlo das ameaças e riscos que causam incidentes.

Importa frisar que a ausência de um suporte que olhe especificamente para os riscos, quer na sua identificação, análise/avaliação e tratamento, é muito preocupante, atendendo a responsabilidade financeira que cada uma das empresas do estudo tem com seus clientes.

Pode-se observar que as medidas de segurança aplicadas, carecem de alguns fatores, como um processo de gestão, a participação de todas as outras áreas que compõem o negócio. A ausência desses fatores e o fraco entendimento sobre questões abrangentes de segurança da informação contribui para a redução da eficácia das medidas aplicadas, atendendo aos objetivos fundamentais de proteção dos ativos de informação de cada organização.

Verificou-se também que os procedimentos de segurança da informação utilizados não são proativos, pois não existe monitorização a nível das infraestruturas tecnológicas, bem como das aplicações que governam os serviços disponibilizados como verificar se as operações estão a ser realizadas no caso de uma operação de transferência, identificar quem a executou, apenas reagem de acordo ao evento.

Uma questão a ter-se em conta é a necessidade da consideração ou envolvimento da segurança da informação na estratégia de negócio para as organizações, pois o contrário inviabiliza a iniciativa de investimentos sobre a segurança da informação, bem como a capacitação dos seus colaboradores quanto a esta temática.

Este estudo permitiu chegar a conclusão de que para as empresas pesquisadas, a maior preocupação ou o ponto crucial para adopção à segurança da informação é evitar perda financeira.

Esta pesquisa tem relevância para as organizações, pois trata de um assunto ainda pouco explorado. Pode ajudar as empresas a terem maior sensibilidade quanto a segurança da informação, implementando os preceitos da ISO 27001, e assim desenvolverem métodos eficazes para a proteção dos seus ativos.

Recomenda-se a realização de outros estudos relacionados com o tema e que englobem aspetos não abordados neste trabalho.

REFERÊNCIAS

Alghathbar, Khaled. (2008). *An approach to establish a Center of excellence in information security*. International Journal of Computer Science and Network Security: USA.

Alves, Magda. (2007). Como escrever teses e monografias: um roteiro passo a passo. 2ª edição – Rio de Janeiro: Elsevier.

Barañano, Ana Maria. (2008). Métodos e Técnicas de Investigação em Gestão: Manual de Apoio à Realização de Trabalhos de Investigação. Ed. Sílabo: 1ª edição, Lisboa.

Beal, Adriana. (2004). Gestão estratégica da informação. São Paulo: Atlas.

Brotby, W. Krag; CISM. (2009). *Information Security Management Metrics: A definitive guide to effective security monitoring and measurement*. Boca Raton: Auerbach.

Bruckman, John Charles; Iman, Steve. (1980) *Consulting with Small Business*: *a process model*. Journal of Small Business Management: Milwaukee.

BS ISO/IEC 27002:2005 (2007). *Code of practice for information security management*: *British Standard*. UK.

Caruso, Carlos A. A. & STEFFEN, Flávio Deny. (1999). *Segurança em informática e de Informações***.** São Paulo: Senac.

Creswell, John (1994). *Research Design: Qualitative and Quantitative Approaches*, Thousand Oaks: SAGE Publications.

Dawel, George (2005). A Segurança da Informação nas Empresas**.** Rio de Janeiro: Editora Ciência Moderna.

Erbschloe, Michael (2005). *Trojans, Worms, And Spyware*: *A computer security professional´s guide to malicious code*. Elsevier.

Gelbstein, Eduardo; Kamal, Ahmad. (2002). *Information Insecurity*: A survival guide to the uncharted territories of cyber-threats and cyber-security. Second Edition: New York.

Gupta, Atul. (2005). *Information systems security issues and decisions for small businesses: an empirical examination*. Information Management & Computer Security**:** USA

Gil, António Carlos. (1991). *Como elaborar projectos de pesquisa*. São Paulo: Atlas.

Magalhães, Hugo; Grilo, Alberto. (2006). A segurança Informática e o Negócio Electrónico. Editor: SPI – Sociedade Portuguesa de Inovações, Porto.

Humphreys, E. (2010) *Information Security Risk Management. Handbook for* ISO/IEC 27001: British Standards Institution, London – UK.

ISO, (2005). ISO/IEC 27001- *Information Security Management System* - Requeriments. International Organization for Standardization: Geneva.

ISO, (2010). ISO/IEC 27001 *for Small Business – Practical advice.* International Organization for Standardization: Geneva.

Krause, Micki; Tipton, Harold F.(1999). *Handbook of Information Security Management*. Auerbach Publications.

Dantas, Marcus Leal (2011). Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos. Olinda: Livro Rápido.

Mcgaughey, J.R.E. et al. (1994) *Implementing information technology for competitive advantage: risk management issues*. Information & Management: USA.

McCumber, J. (2005). *Assessing and Managing Security Risk in IT Systems.* Boca Raton: Auerbach.

Mitnik, kevin D.; Simon William L. (2003). *The Art of Deception*: *Controlling the Human Element of Security*.

Mitnik, kevin D.; Simon William L. (2005). *The Art of Intrusion*: *The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers.* Wiley publishing, Inc. – Indianapolis.

Netto, Abner (2007). Gestão da Segurança da Informação: Fatores que influenciam sua adopção em pequenas e médias empresas. Dissertação de mestrado. Universidade de São Caetano do Sul: Brasil.

NP ISO/IEC 27001:2013 (2013). Sistemas de Gestão de Segurança da Informação – Requisitos. Norma Portuguesa.

Peltier, Thomas R.; Justin, Peltier; Blackley, John (2005). Information Security Fundamentals. New York: Auerbach.

Raggad, Bell G. (2010). *Information Security Management:* Concepts and Practices. Auerbach Publication.

Ramos, Anderson (2008). Security Officer - 1: Guia Oficial para Formação de Gestores em Segurança da Informação. Porto Alegre, RS: Zouk.

Reis, António. (2001). Gestão estratégica dos sistemas de informação. 1ª edição – 1ª impressão – Minerva do Comércio. Lisboa.

Ribas, Carlos Eduardo (2010). Sistema de Gestão de Segurança da Informação em áreas da Saúde. Dissertação de Mestrado – S. Paulo.

Sêmola, Marcos. (2003). *Gestão da Segurança da Informação. Uma visão executiva*: Rio de Janeiro. Campus.

Smith, A.D.; RUPP, W.T. (2002). *Issues in cybersecurity*: *understanding the potential risks associated with hackers/crackers.* Information Management & Computer Security: USA.

Smith, M. (1989). *Computer security*: *threats, vulnerabilities and countermeasures*: Information Age (UK).

Szor, Peter (2005). *The Art of Computer Virus Reserch and Defense*. Addison Wesley Professional.

Takemura, Toshihiko. (2010). *A quantitative study on Japanese worker´s awareness to information security using the data collected by web-based survey*. American Journal of Economics and Business Administration.

Wheeler, Evan (2011). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Elsevier. USA.

Whitman, Michael E.; Mattord, Herbert J. (2010). *Principles of Information Security :Course Technology.* Third edition, Boston – USA.

Yin, R. (2005). Estudo de caso: planeamento e método. Porto Alegre: Bookman.

Sites consultados:

http://www.scis.nova.edu/~cannady/ARES/mitnick.pdf

http://www.infowester.com/malwares.php

http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

http://www.iso27001certificates.com

http://www.bsigroup.com/en-GB/iso-27001-information-security/ISO-27001-for-SMEs

www.fachesf.com.br/pdf/manual_de_seguranca_da_informacao.pdf

http://www.academia.edu/4405328/GIL_Antonio_Carlos_COMO_ELABORAR_PROJETOS_DE_PESQUISA_Copia

http://www.cse.hcmut.edu.vn/~ttqnguyet/download%20ebook%20here!!!/ISSReferences/IS06_Information_Security_Fundamentals.pdf

http://www.bsigroup.ae/upload/MS-Assessment+Certification/General/Documents/BIP0076-Chapter1.pdf

http://www.unirio.br/dtic/sie/copy_of_sie/nivelamento-motivacao

http://www.anip.co.ao/index.php?pag=conteudos&id=67

http://www.academia.edu/4405328/GIL_Antonio_Carlos_COMO_ELABORAR_PROJETOS_DE_PESQUISA_Copia

APÊNDICE A – CARTA DE APRESENTAÇÃO

Luanda, ___ de _____de 2014.

Dissertação de Mestrado: **Gestão da Segurança da Informação:**
Importância da sua Adopção em Pequenas e Médias Empresas Angolanas

Caro Diretor

Frequento o curso de mestrado em Estudos de Gestão na Universidade do Minho e já em fase de dissertação, apresento o tema "gestão da segurança da informação - importância da sua adopção em pequenas e médias empresas Angolanas", que tem como orientador, o Professor Doutor José António Crispim.

Neste contexto, como gestor de TI, venho solicitar a sua colaboração, no fornecimento de informações que servirão de suporte para a realização do Estudo de Caso.

O seu contributo é útil, pois só deste modo, poder-se-á validar algumas hipóteses relacionadas com a gestão da segurança da informação nas organizações.

Declaro que as informações fornecidas serão tratadas com maior sigilo e reservam-se apenas para o trabalho de dissertação.

Com os melhores cumprimentos,

Aluno: Fortunato André
Mestrando em Estudos de Gestão

APÊNDICE B – Ferramentas da pesquisa (entrevista semi-estruturada)

QUESTÕES DO ESTUDO DO CASO

- Idade
- Gênero
- Formação Académica
- Pós Graduação
- Cargo actual exercido na organização
- Tempo no cargo
- Número de funcionários da organização
- Número de funcionários de TI na organização

Gestão da Segurança da Informação

- Que medidas utilizam para protegerem-se das ameaças
- Incidente de segurança da Informação e seu impacto
- A segurança da informação é parte integrante da estratégia de negócio da organização
- Porque adoptam a gestão da segurança da informação

Práticas de Segurança da Informação
Política de segurança da informação
Responsável para concessão, manutenção, revisão e cancelamento das autorizações de acesso à informação.
Existe controlo de acesso lógico.
Existe controlo de acesso físico.
Existe procedimentos para autorização de acesso a informação.
Existe monitorização e controlo das informações nos ambientes lógicos que garantem o acesso apenas as pessoas autorizadas.
As estações de trabalho estão protegidas por uma firewall e um software de antivírus.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados ou instalados.
Existe cópias de segurança.
Existe CPD (centro de processamento de dados).

Política de segurança da informação

- A organização possui política de segurança da informação
- Importância da política de segurança da informação

Gestão de risco de segurança da informação

- A organização possui processo de gestão de risco
- Porque é necessário proteger os ativos de informação
- Procedimentos utilizados para evitar que ameaças exploram vulnerabilidades
- O que compõe um processo de gestão de risco

Práticas de Gestão de Risco de Segurança da Informação
Existe plano de identificação, análise/avaliação e tratamento do risco.
Todos computadores ligados a rede da organização estão protegidos contra ameaças à rede via firewall.
Antivírus configurado para protecção e funcionamento em tempo real.
Existe um local remoto para armazenar as cópias de segurança.
Existe procedimento para que o utilizador informe a área responsável, caso o software de antivírus e a firewall não estejam actualizados ou instalados.
Alerta caso mais de 10% da rede estiver com as definições de vírus desactualizada.
Lista de técnicos credenciados autorizados a entrar no CPD.
Existe plano de contigência para a continuidade de negócio.
A informação da organização é classificada em informação pública, interna geral, interna restrita e confidencial.