Euclides V. Rocha

SEGURANÇA EM SISTEMAS DE INFORMAÇÃO GOVERNAMENTAIS

O Caso do MTIE – Ministério do Turismo, Indústria e Energia

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

28.11.10

Euclides V. Rocha

SEGURANÇA EM SISTEMAS DE INFORMAÇÃO GOVERNAMENTAIS

O Caso do MTIE – Ministério do Turismo, Indústria e Energia

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

28.11.10

Euclides V. Rocha, autor da monografia intitulada Segurança em Sistemas de Informação Governamentais, declaro que, salvo fontes devidamente citadas e referidas, o presente documento é fruto do meu trabalho pessoal, individual e original.

Cidade da Praia aos 30 de Setembro de 2010

Euclides V. Rocha

Memória Monográfica apresentada à Universidade Jean Piaget de Cabo Verde como parte dos requisitos para a obtenção do grau de Licenciatura em Informática de Gestão.

Sumário

Este trabalho monográfico cujo tema é Segurança em Sistemas de Informação Governamentais tem como objectivo avaliar a situação actual dos Sistemas de informação governamental em geral, mais precisamente, no Ministério do Turismo, Indústria e Energia do Governo de Cabo Verde, no que tange à análise e gestão de risco em segurança de informação.

Para materializar-se esse estudo utilizou-se como metodologia consultas Bibliográficas, Entrevistas informal (Conversa aberta), Recolha e Analise de dados.

Pretende-se analisar a situação dos sistemas de informação governamental no que concerne a análise e gestão de risco em segurança de informação, bem como fazer algumas propostas de melhoria dos sistemas e segurança de informação no MTIE e ainda fazer uma recomendação em relação a política da segurança de informação no NOSI.

Dedicatória

Dedico este trabalho monográfico à minha Mãe, meu Pai, Irmão, Irmã pelo incentivo, confiança e força nos momentos de dificuldades para que eu alcançasse mais esta vitória.

"Nenhum pai pode dar
melhor presente aos seus filhos
do que proporcionar-lhes
uma boa educação."
Maomé (s/d) apud Varajão (1998)

Agradecimentos

Não será possível a elaboração de uma obra, sem a contribuição de outrem. Por isso quero expressar a minha profunda gratidão a todos quantos de uma forma ou de outra que contribuíram para o êxito deste trabalho, pois sem as suas contribuições não seria possível o término do mesmo, especialmente o meu orientador "**Jairson Monteiro Santos Mendes**".

Um especial agradecimento a Deus pela vida e saúde que me emprestou, aos meus pais "**Severino Rocha**" e "**Maria L. Pereira Vieira**", meus irmãos e irmãs, tios e tias pelos carinhos e ajudas que me proporcionaram na concretização deste maravilhoso sonho.

Um grande agradecimento ao "**Euclides Horta Rocha**" que sem o seu apoio não seria possível a concretização desta longa caminhada. Obrigado tio.

Agradeço a toda população de "**Rincão**" e a todos colegas da Universidade Jean Piaget de Cabo Verde e em especial aos meus maravilhosos companheiros do curso, pela força e coragem que me deram.

Aos amigos **Janilo**, **Vá-Branca**, **Vá-Batata**, **Da-Costa**, pelos vossos excelentes contributos. Obrigado Maltas.

A todos os colaboradores do **NOSI** e **MTIE**, pela atenção e apoio incondicional que me prestaram durante a realização do trabalho.

À minha família, obrigado pelo vosso carinho.

Conteúdo

Quadros

Figuras

Abreviatura

ANSI – American National Standard Institute.

CIISI – Comissão Interministerial de Inovação para Sociedade de Informação.

CPD – Centro de Processamento de Dados.

CRCV – Constituição da República de Cabo Verde.

CRM – Client Relationship Management.

DMRS – Sistema de Gestão e Recuperação de Documentos.

DoS – Denial Of Service.

ERP – Enterprise Resource Planning.

E-Gov – Governo Electrónico.

IBM – International Business Machines Corporation.

KWS – Sistema de Conhecimento de Trabalho.

LAN – Local Adress Network.

MSI – Modelo da Segurança de Informação.

MTIE – Ministérios do Turismo, Indústria e Energia.

NOSI – Núcleo Operacional para Sociedade de Informação.

PC – Computador.

PDCA – Plan – Do – Check – Act.

PSI – Política da Segurança de Informação.

SAD – Sistemas de Apoio à Decisão.

SAE – Sistema de Automação de Escritório.

SCM – Supply Chain Management.

SGBD – Sistemas de Gestão de Bases de Dados.

SGSI – Sistema de Gestão da Segurança de Informação.

SI – Sistemas de Informação.

SIE – Sistema de Informação para Executivo.

SIG – Sistema de Informação para Gestão.

SUC – Sistema Único de Cobrança.

TI – Tecnologias de Informação.

TPS – Sistemas de Informação Transaccional.

Glossário

Ameaças – Conjuntos de acção ou acontecimentos realizados por pessoas ou não, que pode levar a alteração não desejada de equipamentos dos sistemas de informação.

ANSI – *American National Standard Institute*, ou Instituto Nacional Americano de Padrões – É uma organização formada por grupos da comunidade industrial e comercial dos Estados Unidos, dedicada ao desenvolvimento de normas de produção e comunicação.

Ataque de força bruta – É uma técnica que consiste em testar todas as combinações possíveis de caracteres até encontrar a chave que permita a descodificação do texto cifrado.

Ataque dicionário – É uma técnica baseado em senhas que consiste na cifragem das palavras de um dicionário e posterior comparação com os arquivos de senhas do utilizador.

Ataque DoS – Do inglês *Denial of Service* que significa negação de serviço – Actividade maliciosa utilizado por atacante através de um computador para tirar de operação um serviço ou computador conectado à Internet.

Background – Baixa prioridade; cor de fundo; fundo, segundo plano. Processo ou tarefa que tem um nível de prioridade inferior dentro da alocação de tempo do processador com relação à tarefa executada em primeiro tempo.

Backup – Cópia de segurança – Um arquivo auxiliar, imagem do arquivo fonte, utilizado como base de recuperação de dados quando da ocorrência de um defeito ou perda de dados.

Bancos de dados – Conjuntos formados por várias bases de dados.

Base de dados – Conjuntos de dados, habitualmente muito extensos, com uma determinada estrutura.

Bits – *Binary digit* ou dígito binário – Uma unidade de informação de um equipamento de armazenamento. A capacidade em *bits* é um logaritmo de base dois, do número de possíveis estados do equipamento.

Comércio electrónico – ou e-commerce **–** são transacções comercial onde as partes interagem electronicamente, ou seja, são técnicas e tecnologias computacionais utilizadas para facilitar e executar transacções comerciais de bens e serviços através da Internet.

Data Mining – ou Mineração de dados – é o processo de análise de dados a partir de perspectivas diferentes e resumi-lo em informação útil.

Data Warehouse – é um repositório grande de dados armazenados electronicamente de uma organização, desenhado para facilitar a comunicação e análise.

Drill down – navegar dos dados sumarizados aos dados detalhados.

E-business – é uma aplicação de tecnologias de informação e comunicação no apoio de todas as actividades de negócio.

E-mail – Ou correio electrónico – é sistema de computação que permite a troca de mensagens mediante o uso de modem, ou comunicação de algum tipo de escrita, com envio e recepção usando computador.

Engenheira social – Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do utilizador, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Feed back – Processo de entrada e saída de dados/informação de um sistema.

Gateway – Computador ou material dedicado que serve para interligar duas ou mais redes que usem protocolos de comunicação internos diferentes, ou, computador que interliga uma rede local à Internet (é portanto o nó de saída para a Internet).

Hackers – Programadores tecnicamente sofisticados, que dedicam boa parte do seu tempo a conhecer, dominar e modificar os programas e equipamentos.

Hardware – É componente física de um computador, formado por Rato, Teclado, Monitor e Unidade Central de Processamento.

Interface – Fronteira partilhada entre duas unidades funcionais, definidas pelas suas características físicas comuns de interligação, características dos sinais e outras características apropriadas.

Logoff – Saída ou encerramento da sessão. Procedimento mediante o qual um utilizador encerra uma conexão a um sistema de computador ou dispositivo periférico.

Mainframes – Macro computador – computador de grande capacidade que é normalmente o principal processador de uma organização. Foi designada deste nome após o aparecimento dos mini e micro computadores**.**

Password ou palavra chave – Conjunto de caracteres, de conhecimento único do utilizador, utilizado no processo de verificação da sua identidade, assegurando que ele é realmente quem diz ser.

Problemas semi-estruturados – São problemas que possuem elementos do tipo estruturado e não estruturados. Utiliza a mistura de método standard e juízo humano para a tomada de decisão.

Protocolos - Conjunto de regras e procedimentos técnicos para o intercâmbio de dados entre computadores ligados em rede.

Redes de computadores locais (LAN) – Redes de computadores situadas no domínio privado de um utilizador e limitada geograficamente.

Riscos – São uma expectativa de perda expressada como a probabilidade de que uma ameaça em particular poderá explorar uma vulnerabilidade com um possível prejuízo.

Roteador – Dispositivo de uma rede que recebe dados e os envia aos pontos de destino, sempre usando as rotas mais curtas disponíveis.

Sistema de gestão de bases de dados (SGBD) – Conjunto de aplicações que permite a interacção entre o utilizador e bases de dados.

Site – Local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hiper-texto, que podem conter textos, gráficos e informações multimédia.

Software – Criação intelectual que compreende os programas, procedimentos, regras e qualquer documentação associada, relativos ao funcionamento de um sistema de processamento de dados.

Spam – Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas.

Top-down – Mais geral para mais específicos; descendentes. Significa do mais alto para o mais baixo; do mais genérico para o mais específico.

Unix – Sistema operacional produzido pelos *Bell Laboratories* em 1971 para os minicomputadores DECPDP11, cuja finalidade era proporcionar um meio uniforme e simples em que um número relativamente pequeno de utilizadores, com um considerável grau de inter-relacionamento, pudesse utilizar um só sistema.

Usuário ou utilizador **–** Qualquer pessoa ou entidade que utiliza os serviços de um sistema de processamento de dados.

Vírus electrónico – Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte

de outros programas e arquivos de um computador. Ele depende da execução do programa ou arquivo hospedeiro para que possa se tornar activo e dar continuidade ao processo de infecção.

Vulnerabilidade – É o ponto por onde qualquer sistema está sujeita a sofrer um possível ataque, ou seja, é uma falha encontrada num determinado equipamento, processo e configuração.

Web – Rede, teia, trama, entrelaçamento. Forma abreviada muito frequente para *World Wide Web*. Rede mundial ou um acervo universal de páginas da *Web* interligados por vínculos as quais fornecem ao utilizador informações de um completos banco de dados multimédia, utilizando a Internet como mecanismo de transporte.

Websites – é uma colecção de páginas Web, imagens, vídeos ou outros activos digitais que serão abordados em relação a uma comum caminho raiz em uma rede baseadas em Internet protocolo. Um Web site é hospedado em pelo menos um servidor Web, acessível através de uma rede como a Internet ou uma rede local privada.

Introdução

Com o avanço da ciência e das tecnologias de informação, a questão da segurança em sistemas de informação tem vindo a revelar-se determinante no desempenho adequado das actividades do governo, bem como de qualquer outra organização que tenha como preocupação a salvaguarda das suas informações.

Na perspectiva de Promon Business & Technology Review (2005), hoje em dia, as organizações dependem muito dos sistemas de informação e da internet para desenvolver as suas actividades, (…). Um incidente da segurança pode prejudicar directamente e negativamente as actividades de uma organização, a confiança dos clientes e o relacionamento com outras organizações, ou seja um incidente da segurança pode impedir que as organizações atingem as suas metas e gerar rendimentos para os accionistas.

Esta perspectiva traz a segurança de informação para um patamar novo, não apenas relacionados com a questão da tecnologia e de ferramentas relevante para a protecção da informação mas também como um dos pilares de suporte as estratégias do negócio de uma organização. A gestão de segurança adopta uma nova postura, levando em conta os elementos estratégicos de uma organização e evolui para a extensão da prática de gestão de riscos do negócio. (Idem, 2005)

A segurança em sistema de informação, é hoje considerada um importante instrumento para a melhoria da competitividade e de desenvolvimento de qualquer organização. Actualmente

esta modalidade ganhou novas perspectivas no campo das organizações, e passou-se a destacar como um excelente instrumento para a dinamização e o desenvolvimento dos serviços administrativos do governo. Aparece como uma solução ao combate aos ataques dos piratas informáticos, às invasões dos vírus informáticos, os roubos da informação, os acessos não autorizados, isto é, um verdadeiro mecanismo de suporte às actividades das organizações.

Cabo verde, como um país de desenvolvimento médio, a questão da segurança em sistemas de informação no governo tem sido muito importante para o desenvolvimento das actividades económicas bem como para melhorar a segurança a nível interno e externo das organizações. Por conseguinte essa segurança é uma das apostas firmes do governo, fazendo parte do plano estratégico de desenvolvimento. Neste contexto enquadra-se este trabalho, com o intuito de aperceber a situação actual dos Sistemas de Informação Governamental em geral, mais precisamente, no Ministério do Turismo, Indústria e Energia do Governo de Cabo Verde, no que tange à análise e gestão de risco em segurança de informação.

1 Objectivos:

Para a elaboração deste trabalho foram definidos os seguintes objectivos:

1.1 Objectivo Geral

- Avaliar a situação actual dos Sistemas de informação governamental, mais precisamente, no Ministério do Turismo, Indústria e Energia do Governo de Cabo Verde, no que tange à análise e gestão de risco em segurança de informação.

1.2 Objectivos Específicos

- Compreender o conceito dos Sistemas de informação e a sua importância para a organização/instituição.

- Descrever a evolução histórica dos Sistemas de informação e os principais tipos de sistemas de informação.

- Explicar os principais aspectos da segurança em Sistemas de informação, bem como as suas políticas e planos de segurança.

- Explicar as etapas de análises de risco e sistemas de gestão da segurança de informação, bem como os tipos de risco existentes.

- Conhecer a situação da segurança de informação no Ministério do Turismo, Indústria e Energia – MTIE.

- Propor melhorias da segurança em Sistemas de informação no MTIE caso necessário.

2 Metodologia

Para a realização deste trabalho optou-se pela **abordagem qualitativa**, através de consultas bibliográficas como livros, artigos e sites da internet, visto que para a elaboração de qualquer trabalho científico primeiramente tem que ter suporte teórico que serve de alicerce a parte prática – **Análise documental.**

Optou-se ainda por **observação indirecta**, da instituição em estudo como forma de recolher informação considerada pertinente para a construção do mesmo. Esta observação foi realizada mediante a solicitação dos directores dos diferentes departamentos da organização.

Também utilizou-se uma **abordagem quantitativa**, tendo em conta que optou-se por fazer um "***Case study***" onde foram realizados entrevista informal (conversa aberta), análise e recolha de informações da organização, com o objectivo de aperceber a situação da segurança em sistema de informação no Ministério do Turismo, Indústria e Energia de Governo de Cabo Verde – **Entrevista informal (Conversa aberta), Recolha e análise de dados.**

3 Estrutura

O presente trabalho encontra-se estruturado em quatros Capítulos começando pela abreviatura, glossário e uma introdução, onde faz-se referência ao enquadramento do trabalho, justificação da escolha do tema, os objectivos e a metodologia utilizada.

No Primeiro Capítulo, abarca-se as grandes directrizes do **Sistema de informação,** nomeadamente alguns conceitos, contributos de **SI** na organização, breve história da evolução do **SI**, e por último os diferentes tipos do **SI**.

No Segundo Capítulo, apresenta-se a **Segurança em sistemas de informação,** onde fala-se da segurança de informação e suas características na perspectiva de vários autores, de seguida faz-se uma breve abordagem sobre os tipos da segurança de informação onde debruça-se sobre a segurança lógica e física sendo este último com maior destaque. Dentro da segurança física foram abordados os seguintes pontos: Segurança dos recursos humanos ou pessoas, onde ainda dentro deste assunto trata-se da questão de formação e sensibilização dos utilizadores e o processo de recrutamento do pessoal como elemento importante da segurança de organização. Aborda-se ainda assunto como segurança dos centros de processamentos de dados e/ou instalação e por último segurança dos equipamentos.

De seguida apresenta-se a análise de risco em segurança de informação, onde dentro deste assunto destaca-se alguns conceitos considerado importante para a compreensão do mesmo, fala-se dos diferentes tipos de riscos, as principais etapas de análises de riscos e por último o sistema de gestão da segurança de informação.

Também apresenta-se as políticas da segurança de informação, onde debruça-se sobre conceitos e algumas perspectivas de políticas da segurança de informação, fala-se da política de segurança de *Password*, de *Email*, de acesso a internet e de uso de estação de trabalho.

Trata-se ainda do planeamento da segurança de informação, destacando-se os tipos de planos da segurança de informação, onde dentro deste assunto aborda-se especificamente os planos de contingências, sendo este constituído por mais três tipos de planos de segurança: o plano da administração de crise, o plano de continuidade operacional e o plano de recuperação de desastre.

No Terceiro Capítulo, dedica-se especificamente ao título do trabalho **Segurança em sistema de informação governamental,** onde debruça-se sobre conceito do governo, sistema de informação governamental. Dentro deste último destaca-se os diferentes tipos de sistemas de informação governamental.

De seguida fala-se da segurança em sistema de informação governamental de uma forma em geral e por último a segurança do sistema de informação governamental em Cabo Verde.

No Quarto Capítulo, descreve-se uma situação "***Case study",*** onde foram caracterizados o local em estudo. Na caracterização do local em estudo foram caracterizados a Instituição em si, as infra-estruturas tecnológicas, os sistemas de informação, e por último a política de segurança da Instituição.

Faz-se uma análise profunda dos dados recolhidos, e para terminar faz-se a proposta de melhoria, a recomendação, a conclusão e as referências bibliográficas.

Capítulo 1: Introdução aos sistemas de informação

1 Contextualização

Ao falar-se dos sistemas de informação emerge a seguinte questão: Quais as actividades que fazem parte de um sistema de informação? No entanto, para melhor compreender o conceito dos sistemas de informação e sua importância definiu-se alguns conceitos que estão inteiramente relacionados com ela e que sem o qual este não funciona.

Sistema – é um conjunto de elementos interligado entre si, funcionando como um todo, de forma a atingir um objectivo em comum, caracterizados por uma entrada (*inputs*), produzindo resultados (*outputs*), organizados numa determinada organização. (Rascão, 2001)

Dados – são factos ou eventos, imagens ou sons identificado no seu estado bruto que pode ser importante para a realização de uma actividade, mas que por si só, não produzem informação, ou seja, não conduz a compreensão do mundo que nos rodeias. (Idem, 2001)

Informação – dados organizados e dotados de uma certa importância e objectivos para a pessoa ou organização que a detêm (Drucker, 1988) apud Lopes et al (2005). Ou ainda podem

ser dados organizados com determinadas regras ou padrões e com significados para a pessoa ou organização que a detêm. (Davis & Botkin, 1994) apud Lopes et al (2005)

Segundo Rodrigues (2002) dado e informação são dois conceitos que relacionam entre si, mas são diferentes, isto porque os dados – são, eventos separados, representações não estruturadas cuja utilização poderá ser importante ou vantajoso numa determinada posição. Enquanto, informação – é o resultado da interpretação dos dados. O autor vai mais além afirmando que segundo Varajão (1998) a informação – é um grupo de dados que quando colocados num contexto útil e importante é uma mais-valia para tomada de decisão da pessoa ou organização que a detêm.

> Na mesma perspectiva defende Varajão (1998) que *"apesar destes dois conceitos são em termos de significados diferentes, eles estão directamente relacionados. A sua ligação é similar à relação entre matéria-prima e o produto final obtido a partir da mesma, ou seja, os dados não são informação até que sejam processados e organizados de modo a possibilitar a sua compreensão e utilização."*

Partindo da ideia do autor acima referido, isto quer dizer que os dados e a informação são dois conceitos que derivam entre si, isto é, não existe informação sem antes existirem os dados, e os dados existem por si só independentemente de existirem informação. Dados para serem informação tem que passar por um processo de transformação. Para melhor compreender a diferença entre dados e informação analisa-se a figura abaixo:

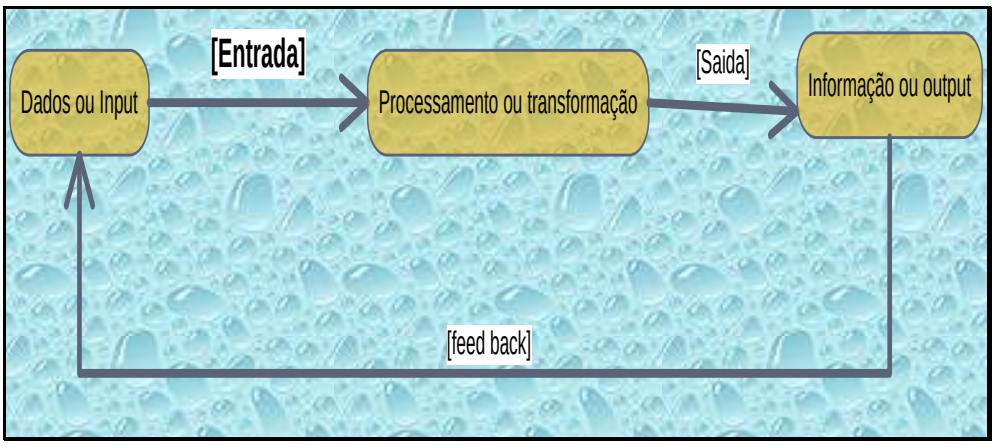

Figura 1 – Actividades dos sistemas de informação

Na figura acima apresentado vê-se que o sistema de informação é composto por uma entrada de dados, ou *input*, no seu estado bruto, onde estes são processados ou transformados através de um conjunto de tecnologias de informação, e que depois é apresentado para o exterior em forma de *output* ou informação. Este processo de entrada e saída de dados/informação se dá através do mecanismo de *feed back*.

Paralelamente a este assunto, pode-se ainda dizer que para além dos sistemas de informação serem constituídos pelo conjunto de actividades acima mencionados, também são constituídos por um conjunto de componentes que segundo Gouveia (s/d) são: Informação; Recursos humanos ou Pessoas; hardware e software ou Tecnologias de Informação; Armazenamento de Dados; Dados e Comunicação. A figura que se segue indica de forma clara e resumidas os principais componentes de um sistema de informação:

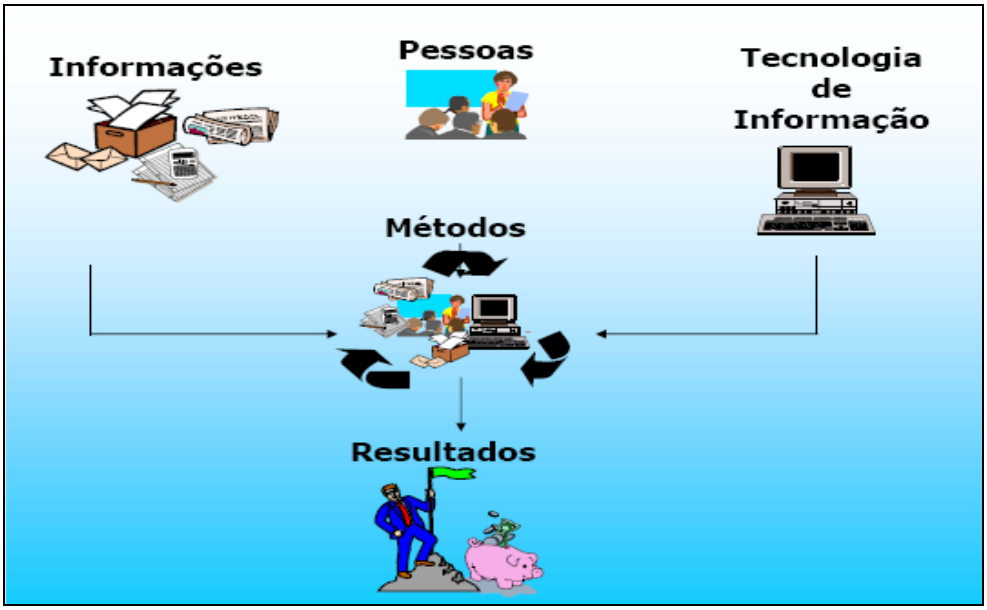

Figura 2 – Componentes dos sistemas de informação

FONTE: LUZ, Carlos (2009) Disponível: <http://moodle.cv.unipiaget.org/course/view.php?id=44 > [Consultado em 22-04-2010]

Segundo Varajão (1998) Sistema de Informação, Tecnologia de Informação e Informação, são expressões que estão na "ribalta", mas contudo, apesar de serem termos muito banais carecem de entendimento universal, (…) por isso, é importante apresentar um conjunto de conceitos e reflexão sobre a importância de informação e sistemas de informação na organização,

identificando alguns dos seus aspectos principais através de definições simultaneamente rigorosas e próximas do que é comummente aceite.

Tecnologias de informação (TI) – são conjuntos de *hardware* e *software* interligadas entre si de forma a recolher, processar, armazenar, procurar e disponibilizar informação. (Isaías, 2001)

Sistemas de informação (SI) – É um sistema que recolhe, processa, armazena e distribui informação relevante para a organização (…) de modo que a informação seja acessível e útil para aqueles que dela necessitam incluindo gestores, funcionários, clientes (…). Um sistema de informação é ainda um sistema de actividade humana (social) que pode ou não envolver a utilização de computadores. (Buckingam, 1987) apud Lopes, et al (2005)

O avanço na sociedade de hoje exige uma nova forma de estruturar a organização, e uma das formas de acompanhar essas mudanças passa pela introdução dos sistemas de informação na organização como forma de agilizar e dar resposta eficientes/eficazes a sociedade. Dai que considera-se importante destacar o contributo dos sistemas de informação na organização.

1.1 Contributo dos sistemas de informação na organização

Do ponto de vista do autor Rascão (2001) a relação entre o negócio e o **SI** está a aumentar cada vez mais, pois estes podem gerar oportunidades de negócio e criar vantagens competitivas, visto que cada dia que passa existe uma maior penetração das tecnologias da informação e da comunicação nas organizações, (…).

Defende Lopes, et al (2005) que ao falarmos dos sistemas de informação pensamos a priori em organização e informação, isto porque, existem uma relação de dependência entre elas, ou seja não existe organização sem informação e nem sistema de informação sem informação.

Para Freitas et al (2001) & Lopes et al (2005) os **SI** permitem a organização:

- Atingir os seus objectivos, através da recolha, armazenamento, processamento e distribuição da informação;

- Lidar com representações simbólicas da organização, ou seja, com a informação incluindo o trabalho da organização do tipo funcional.

- Melhorar a tomada de decisão da organização, transformando a informação num elemento crucial para a sobrevivência da organização;

- Auxiliam as organizações a suprirem as necessidades de informação interna e externa em curto espaço de tempo, devido a rápida transformação do mercado.

Na mesma perspectiva reforça o autor Luz (2009) que o **SI** ajuda:

- As organizações ou indivíduos a melhorar os produtos ou os processos da organização;

- Permitem que uma organização funcione como uma unidade onde vários sistemas são coordenados, e os mesmos dados estão representados da mesma forma em sistemas diferentes. Existe uma integração entre os sistemas, quando necessária;

- Focalizam o processamento de dados centrado nos objectivos dos negócios e oferecem a possibilidade de modificar procedimentos computadorizados rapidamente;

- Controlam as informações de tal forma que os principais responsáveis pela tomada de decisão possam ter as informações disponíveis na sua melhor forma.

De acordo com Lopes, et al (2005) os **SI** assumem nos dias de hoje um papel preponderante para mudança organizacional. (…) Elas acrescentam valor à mudança, oferecendo várias possibilidades para organizar e reorganizar o trabalho na organização.

> *"Um sistema de informação deve suportar as necessidades de informação de todos os níveis de decisão da organização, sendo, consequentemente, necessária ter em consideração a existência de vários tipos e necessidades específicas de informação, cujas contribuições, em termos de valor para o negócio, são bastantes diferentes."* (Varajão, 1998)

A ideia do autor acima referenciado leva-se dizer que os sistemas de informação constituem o elemento de extrema importância para o desenvolvimento de qualquer organização isto porque o sucesso ou insucesso de uma organização depende do seu sistema de informação.

Em nota de resumo constata-se que hoje em dia os sistemas de informação fazem parte das organizações, transformando-se num instrumento vital desta; então cabe a cada organização decidir a composição dos sistemas de informação e a mobilizar-lhes de forma a atingir os seus objectivos.

2 Evolução dos sistemas de informação

O estudo da evolução dos sistemas de informação é de grande interesse, sobretudo para a organização. O **SI** é um tema bastante complexo e, ao mesmo tempo, um dos mais importantes para os gestores e decisores. Tendo em conta a importância do sistema de informação na organização, faz-se uma breve análise sobre a sua evolução histórica, bem como os diferentes tipos de sistemas de informação.

Segundo Falsarella & Chaves (2008) o Século XX é marcado pelo advento da Era da Informação, onde a informação expandiu de forma muito rápida. Desde a invenção do telégrafo eléctrico em 1837, passando pelos meios de comunicação de massa, e até mais recentemente, o surgimento (…) da Internet, o ser humano tem de lidar e conviver com um crescimento acelerado de grande quantidade de dados disponíveis.

De acordo com o ponto de vista dos mesmos autores antes da vulgarização dos computadores, os sistemas de informação nas organizações se baseavam basicamente em práticas de arquivamento e recuperação de informações de grandes repositórios. Existia a figura do "arquivador", que era o principal organizador dos dados, (…) quando necessário fazê-lo.

> Ainda defende esses mesmos autores, *"que esse método, apesar de simples, exigia um grande esforço para manter os dados actualizados bem como para recuperá-los. As informações em papéis também não possibilitavam a facilidade de cruzamento e análise dos dados. Por exemplo, o inventário de stock de uma empresa não era uma tarefa trivial nessa época, pois a actualização dos dados não era uma tarefa prática e quase sempre envolvia muitas pessoas, aumentando a probabilidade de ocorrerem erros."* (Idem, 2008)

No entender de Isaías (2001) até à década de 80, o poder de computação nas organizações encontrava-se concentrado e a informação separada e espalhada. Na prática os mainframes eram o principal responsável pelo processamento de toda a informação e existiam terminais que não possuíam capacidade de processamento nos quais os utilizadores faziam os seus trabalhos.

Afirma ainda o autor que *"actualmente a tendência é que o poder de computação nas organizações se encontre descentralizado e a informação seja partilhada pelos diversos utilizadores nas organizações"*.

> No ponto de vista de Varajão (1998) *"(…) os sistemas de informação consistiam apenas no processamento manual de dados para apoio do processo de decisão, o papel (relatórios dactilografados ou manuscritos), era o principal suporte da informação. No entanto, após o desenvolvimento do primeiro computador comercial na década de cinquenta (1951), o computador passou a assumir o processamento de dados, fazendo o uso das grandes capacidades de cálculos e armazenamento que foram sendo desenvolvidas."*

As ideias dos autores acima referidos são convergentes e permitem formular o seguinte resumo: antes de existirem os computadores já existiam **SI**, mas só que traziam junto muitas dificuldades. Contudo com o advir dos computadores tudo ficou mais fácil de analisar, processar, recuperar e disponibilizar informação por parte das pessoas e organizações.

Para melhor compreender a evolução do sistema de informação o autor Varajão (1998) no seu livro planeamento de sistema de informação, e o autor Freitas et al (2001) propõe-nos uma

figura que apresenta a evolução dos diferentes tipos de sistemas de informação, (sobre tipos do sistemas de informação iremos aprofundar mas adiante neste capítulo) bem como a época dominante de cada um.

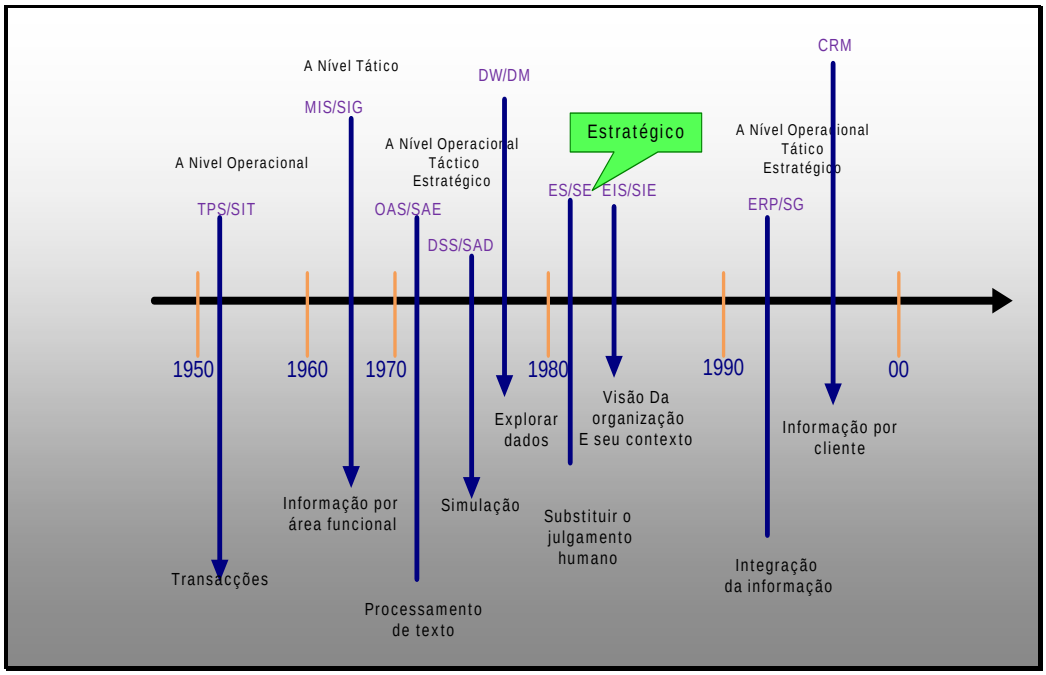

Figura 3 – Evolução dos sistemas de informação

FONTE: FREITAS et al (2001) & VARAJÃO (2002)

Importa-se relembrar que a figura aqui analisada foi uma compilação feita de duas figuras proposto por Varajão e Freitas acima referidos.

Em suma concluí-se que os sistemas de informação tiveram uma evolução muito rápida entre 1950 a 1990. Da observação feita a figura, pode-se ver que entre o ano (1950) e (1960) surgiu o sistema de processamento transaccional focalizada ao nível operacional; entre o ano (1960) a (1970) surgiu o sistema de informação para gestão focalizada ao nível táctico.

Nos meados de anos (1970) e (1980), surgiram os sistemas de automação de escritórios; o sistema de apoio a decisão; e os data *warehouse/data mining* focalizada ao nível operacional, táctico e estratégico.

Entre os meados de anos (1980) e (1990) surgiram os sistemas de informação para executivos; o sistema de informação para especialista focalizado ao nível estratégico. A partir do ano (1990), surgiram o sistema de gestão empresarial e o *client relationship management* (CRM) focalizado ao nível operacional, táctico e estratégico. Apoiado na ideia Freitas et al (2001).

3 Tipologias dos sistemas de informação

De acordo com Chaves & Falsarella (s/d) existem várias formas de classificar os sistemas de informação. No entanto dessas formas o autor Luz (2009) destacou algumas delas como por exemplo:

Classificação do SI de acordo com a estrutura organizacional que engloba (sistemas de informação departamental, sistemas de informação inter-empresas, sistemas de informação empresarial).

Classificação do SI de acordo com a área funcional (sistemas de informação que actua a nível departamental, que suporta as áreas tradicional da organização).

Classificação do SI de acordo com a arquitectura dos sistemas (sistemas baseados num computador central, sistemas baseados em computador pessoal, sistemas baseados em sistemas distribuídos ou em redes).

Classificação do SI de acordo com os processos de *negócio* *client relationship management* (CRM*), supply chain management* (SCM), *enterprise resource planning* (ERP)).

Defende ainda Luz (2009) que os SI podem ainda ser **classificado de acordo com o tipo de apoio** fazendo parte destes sistemas:

3.1 Sistemas de informação transaccional (TPS ou SIT)

É o primeiro sistema desenvolvido e utilizados actualmente pela maioria das organizações, pois tem grande importância para a organização isto porque suporta as actividades tais como

monitorar, colectar, armazenar processar e distribuir os dados da empresa, e as transacções centrais como compra de material, controlo de *stock* e outras operações realizados dentro da organização servindo como base para outros sistemas existindo dentro do mesmo. (Freitas et al 2001),

Diz Laudon & Laudon (2001) apud Bazzotti & Garcia (s/d) que um (**TPS)** é um sistema computadorizado que está ligado a execução das transacções repetitivas e rotineiras da empresa de modo a agilizar e facilitar a resolução dos trabalhos. Este tipos de sistema disponibiliza informação do tipo rotineiro como o caso de folha de pagamentos, notas fiscais e relatórios exigidos pela empresa.

De acordo com Luz (2009) os objectivos principais do **TPS** são:

- Processar dados gerados por e sobre transacções, ou seja, capturar, processar, armazenar transacções e produzir vários documentos relacionados às actividades comercias;

- Manter um alto grau de precisão, ou seja, processamentos de dados sem erros, e ainda produzir relatórios e documentos em tempo real aumentando a eficiência do trabalho;

- Assegurar a integridade dos dados e da informação, ou seja, assegurar que todos os dados e informações armazenados nas bases de dados estejam exactos, actuais e apropriados;

> Na mesma perspectiva defende Boghi & Shitsuka (2002) que *"o objectivo principal do **TPS** é apoiar à operação e processar os dados de transacções dos negócios das organizações. (…) Neste tipo de sistemas os dados transaccionados são normalmente simples, como é o caso de telas de colectas de dados relatórios simples os quais não envolvem muita complexidade. Os bancos de dados são abastecidos com os dados transaccionais e geram-se relatórios simples para o pessoal operacional realizar suas tarefas."*

Para Beuren & Martins (2001) "*um **TPS** bem sucedida será uma excelente base de dados de apoio a entrada aos outros sistemas de informação. O **TPS** é a base que sustenta a integridade e a precisão da informação gerada, assegurando a confiabilidade dos sistemas de informação hierarquicamente acima dele*".

3.2 Sistemas de informação para gestão (SIG ou MIS)

Para Stair (1998) apud Beuren & Martins (2001) um sistema de informação para gestão **(SIG)** é um grupo organizado de pessoas, procedimentos, bases de dados e dispositivos utilizados para disponibilizar informações de rotina aos administradores e tomadores de decisões.

> De acordo com Silva (s/d) "***SIG** tratam das transacções consideradas essências para os gestores, compara as transacções com um plano de acção, sendo fundamentais, na disponibilização de informação correctas e no momento exacto para a tomada de decisão dos gerentes. (…). O **SIG** ainda ajuda a reduzir os custos do crescimento e torna possível às empresas operarem, em grande escala, com aumentos mínimos nos custos de coordenação e gestão."*

Silva (s/d) no seu trabalho de pesquisa conclui que o **SIG** possui um conjunto de funções e características tais como:

- Integrar dados de diversas aplicações e transformá-los em informação, fornecendo-as para o planeamento operacional, táctico e estratégico da organização;

- Suprir gerentes com informações para que estes possam comparar o desempenho actual da organização com o que foi planeado;

- Produzir relatórios que auxiliem os gerentes na tomada de decisões.

Também defende Boghi & Shitsuka (2002) que o **SIG** incluem o planeamento, a coordenação e o controlo, isto é, fornecem informações gerais dos sistemas orientados para operação. Os relatórios, telas ou transacções são relativamente simples e em formatos preestabelecidos.

Ao fazer uma análise comparativa entre **TPS** e **SIG**, pode-se concluir que a principal diferença existente é que o **TPS** tem a visão da organização a partir de cada operação com cada cliente quer interno ou externo a organização, enquanto o **SIG** busca agregar os dados de determinada operação, fornecendo informações consolidadas sobre aquela operação num determinado período de tempo, para que o gerente tenha uma ideia clara e geral daquele tipo de operação. (Freitas et al, 2001)

3.3 Sistemas de automação de escritório e sistema de conhecimentos do trabalho

Segundo Freitas et al (2001) com o advir da era tecnológicos e de informação sentiu-se necessidade de automatizar os serviços realizadas nos escritórios, surgindo assim, os sistemas de automação, que ajudariam tanto os executivos da organização, como todas as pessoas envolvidas em tais actividades. Ainda os autores afirmaram que a automação das tarefas dos escritórios trouxeram consigo rapidez de resposta para a organização, focalizando assim a busca e comparação de diversos alternativos para o mesmo problema, (…) surgindo assim o sistema de apoio a decisão que falaremos mais adiante".

Laudon & Laudon (2001) apud Bazzotti & Garcia (s/d) definem sistemas de automação de escritório (**SAE**) como sendo conjunto de aplicação informática desenvolvido para aumentar o rendimento dos trabalhadores de dados, de modo a suportar à coordenação e a comunicação de um escritório típico.

De acordo com Boghi & Shitsuka (2002) o **SAE** tem como objectivo a automação das tarefas administrativas, melhorando a comunicação e a produtividade no escritório. Esses sistemas incluem as redes de computadores locais, os sistemas administrativos e o uso de aplicativos de automação.

A semelhanças dos sistemas de automação de escritório o sistemas de conhecimento do trabalho (**KWS**) é segundo Luz (2009) sistemas cuja função principal é a integração de novos conhecimentos nos negócios e ajudar a organização a controlar o fluxo de papel.

3.4 Sistemas de apoio à decisão (SAD ou DSS)

Segundo Batista (2004) apud Bazzotti & Garcia (s/d) (**SAD)** são conjuntos de sistemas que interagem entre as acções de usuário, disponibilizando dados e modelos para a solução de problemas semi-estruturados, focando a tomada de decisão ou seja disponibilizam recursos considerados vitais para a realização de suporte às decisões do nível de gestão.

De acordo com Pereira (2006) **SAD** são sistemas complexos que auxiliam os decisores a intervir em diferentes panoramas de negócio da empresa ou ainda permite a organização a possibilidade de simular previsões com base no percurso histórico da organização e para além de escolher a melhor solução para a organização.

Para além de **SAD** possuir capacidade de reconciliar tecnologias de informação a conhecimento humano, é um sistema capaz de apoiar a análise de dados *ad hoc* e modelação de decisão para a definição de um projecto futuro, e em intervalos irregulares e não planeados. (Moore & Chang, 1980) apud (Aronson & Turban, 2001) apud Pereira (2006)

Segundo Silva (2005) Os **SAD** ao contrário de **SIG** baseia-se em [1]modelos e bancos de dados como elementos indispensáveis dos sistemas.

3.5 Sistemas de suporte ao executivo (ESS ou SIE)

Ao contrário de **SAD** um (**SIE)** é segundo Boghi & Shitsuka (2002), um sistemas que consolidam informações de fontes internas e externas das empresas. Este sistema fazem uso

[1] "**Uma base de modelo de sistemas de apoio à decisão** - é um componente de software que consiste em modelos utilizados em rotinas computacionais e analíticas que expressam matematicamente relações entre variáveis. Os pacotes de software de sistemas de apoio à decisão podem combinar componentes de modelos para criar modelos integrados de apoio a tipos específicos de decisões." Silva (20005)

de formas gráficas de apresentação de resultados, são pouco ou mesmo não estruturados e caracteristicamente são utilizados pela alta administração de uma empresa. Os dados para utilização nesses sistemas são seleccionados a partir de "*drill down*" de bancos de dados de outros sistemas já mencionados acima.

Segundo Furlan, Ivo & Amaral (1994), apud Beuren & Martins (2001) os **SIE** possuem as seguintes características:

- Possuem apresentação de dados através de recursos gráficos de alta qualidade, recuperam informações de forma rápida para a tomada de decisão e ainda destinam-se a atender às necessidades de informação dos executivos;

- Oferecem facilidade de uso, intuitivo, não necessita de treino específico em informática e são desenvolvidos de forma a adaptar-se na cultura da empresa e no estilo de tomada de decisão de cada executivo;

- Filtram, resumem, acompanham e controlam dados ligados aos indicadores de desempenho dos factores críticos de sucesso e proporcionam acesso a informações detalhadas subjacentes às telas de sumarização organizadas numa estrutura *top-down*.

- Utilizam informações do ambiente externo (concorrentes, clientes, fornecedores, indústrias, governo, tendências de mercado).

Também numa abordagem comparativa entre **SAD** e **SIE**, anota-se alguma diferença que de acordo com Henry C. Lucas Jr. [LUCA90], apud Chaves & Falsarella (2008) o que diferencia em geral um **SIE** em relação a **SAD** é a sua interface com o usuário, que deve permitir que um executivo utilize esse sistema com facilidade.

A figura abaixo evidência de forma clara e sintetizadas os diferentes tipos de sistemas de informação classificado segundo o tipo de actividade que apoia.

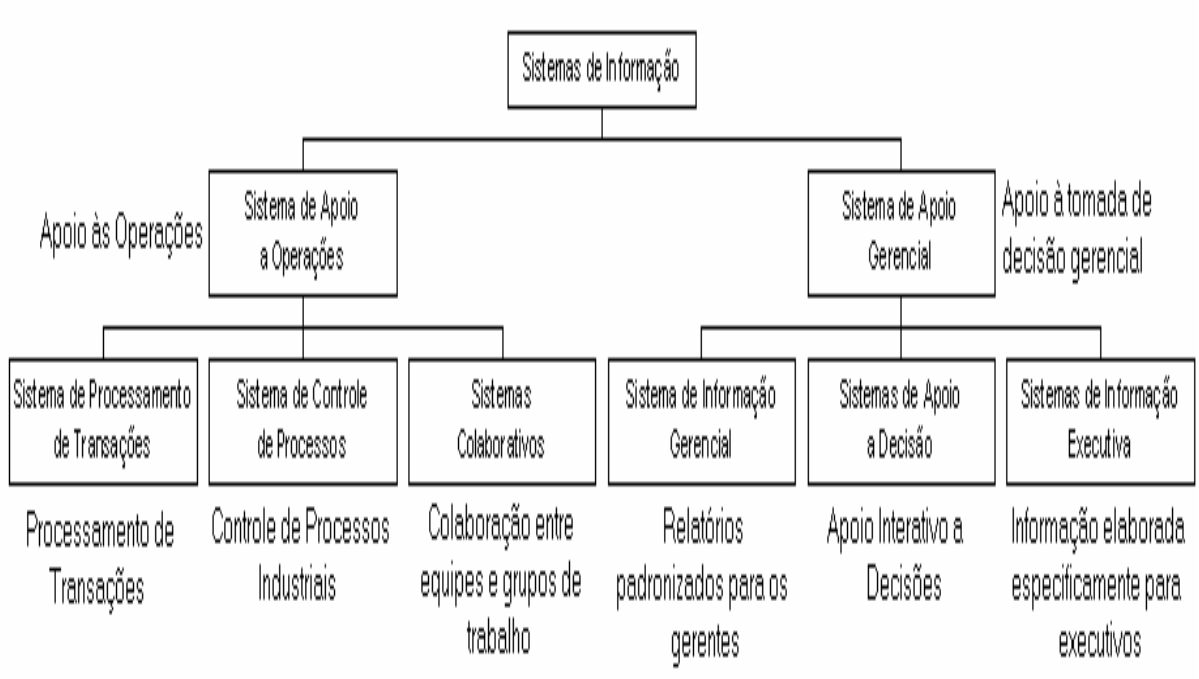

Figura 4 – Classificação dos sistemas de informação segundo a actividades que apoiam

FONTE: O'brien (2002) apud SILVA, Cristiano (2005)

Da análise a figura acima pode-se ver os diferentes tipos de sistemas de informação acima mencionados e outros que ainda não foram mencionados aqui. Isto dá-se a entender que existem vários tipos de sistemas de informação[2].

[2] É de referir que quando fala-se dos tipos dos sistemas de informação não será tarefa fácil, tem diferente apreciação, isto porque cada autor classifica os sistemas de informação de acordo com os seus critérios.

Capítulo 2: A Segurança em sistema de informação

1 Enquadramento

Este capítulo versa sobre a segurança em sistema de informação onde apresenta-se a segurança de informação e suas características na perspectiva de vários autores, de seguida faz-se uma breve abordagem sobre os tipos de segurança de informação onde debruça-se sobre a segurança lógica e física sendo este último com maior destaque. Dentro da segurança física foram abordados os seguintes pontos: Segurança dos recursos humanos ou pessoas, onde ainda dentro deste assunto trata-se da questão de formação e sensibilização dos utilizadores e o processo de recrutamento do pessoal como elemento importante da segurança de organização. Aborda ainda assunto como segurança dos centros de processamentos de dados e/ou instalação e por último segurança dos equipamentos.

De seguida apresenta-se a análise de risco em segurança de informação, onde dentro deste assunto destaca-se alguns conceitos considerado importante para a compreensão do mesmo, fala-se dos diferentes tipos de riscos, as principais etapas de análises de riscos e sistema de gestão de segurança de informação.

Também apresenta-se as políticas de segurança de informação, onde aborda-se sobre conceitos e algumas perspectivas de políticas de segurança de informação, fala-se da política de segurança de *Password*, de *Email*, de acesso a internet e de uso de estação de trabalho.

Trata-se ainda do planeamento de segurança de informação, destacando-se os tipos de planos de segurança de informação, onde dentro deste assunto aborda-se especificamente os planos de contingências, sendo este constituído por mais três tipos de planos de segurança: o plano de administração de crise, o plano de continuidade operacional e o plano de recuperação de desastre.

2 Segurança de informação e suas características

Partindo do pressuposto que a organização de hoje está confrontada com problema da segurança em toda área do negócio devido a rápida transformação tecnológica, foi apresentado aqui as propriedades consideradas importantes para a segurança de qualquer organização.

> Na óptica de Torres et al (2003) *"a segurança deverá ser pensada em moldes concêntricos e de profundidade, com vista a incrementar os níveis de protecção contra acessos não autorizados. Segundo esta lógica, os bens mais preciosos deverão encontrar-se mais perto do centro das instalações, obrigando à passagem por diversos níveis de validação. Pelo contrário, os componentes menos valiosos ou mais facilmente substituíveis, poderão ficar em zonas periféricas, menos protegidas, mas nunca dispensando por completo um qualquer tipo de salvaguarda."*

Segundo Mamede (2006) a segurança não é um processo estático mas sim um processo que está em constantes mutações e de difícil gerir e controlar. Ela está associado a risco e à prevenção do mesmo, ou seja, a segurança é a capacidade que temos para prevenir que as ocorrências indesejadas se concretiza ou pelo menos tentar minimizar que acção mal intencionada ou indesejado se causarem estrago maior aos nossos sistemas.

No entender do Boghi & Shitsuka (2002) não pode-se falar da segurança de informação sem antes levar em conta as questões tais como: a segurança contra vírus de computadores, a segurança contra furtos de informação, equipamentos, software, a segurança contra fraudes informatizadas, o trabalho de auditorias de computador, a segurança contra pirataria, os aspectos da informática associada a disputas jurídicas e outros aspectos de segurança contra infortúnios em informática (…) etc.

Para evitar ou minimizar estes problemas, todos os utilizadores do sistema de informação devem ter conhecimento sobre o objectivo da segurança de informação de qualquer organização.

> Deste modo afirmar Clesio (2008) que a "***Segurança de Informação*** *– é a protecção das informações de uma empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto as pessoais podendo este ser afectada por factores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca, ou por pessoas mal intencionadas que têm o objectivo de furtar, destruir ou modificar tal informação."*

Nesta linha de pensamento, leva-se dizer que um dos objectivos da segurança de informação é a protecção das informações e activos de uma organização ou empresa contra os furtos ou ataques proporcionados com ou sem intenção de prejudicar a organização. Portanto é da responsabilidade de qualquer organização proteger os seus activos contra qualquer males que possam surgir.

Contudo a solução adequada da segurança de informação passa pela satisfação das várias características que segundo Monteiro et al (2000) alguns dos mais reconhecidos são as seguintes: **A Autenticação, Confidencialidade, Integridade, Controlo de Acesso, Não – repudiação e Disponibilidade.** A figura abaixo ilustra de forma clara a relação existente entre algumas delas:

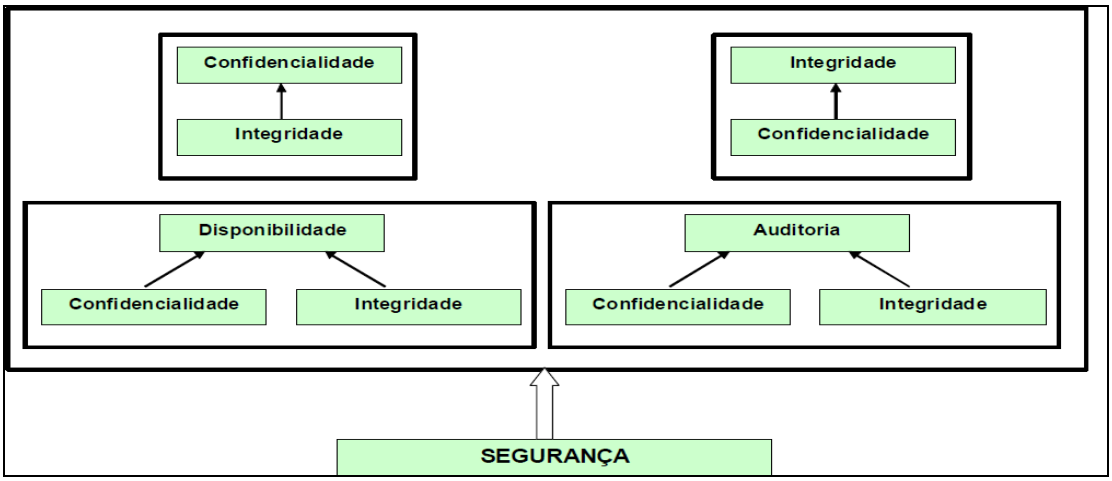

Figura 5 – Características da segurança de informação

FONTE: LAUREANO, P. A. Marcos. (2005)

É evidente que todas essas características são, interdependentes entre si, devendo a sua conjugação ser feita passo-a-passo, de acordo com as necessidades da segurança específicas da rede que, por sua vez, são condicionadas pelos objectivos e natureza da organização que a detém. (...) (Monteiro et al, 2000)

Segundo Laureano (2005) a confidencialidade depende da integridade ou seja se perdemos a integridade de um sistema, automaticamente o mecanismo que confere a confidencialidade deixa de ser confiáveis. Assim também o é, com a integridade e confidencialidade, se perdemos a informação considerada confidencial como por exemplo a senha do administrador de sistema o mecanismo de integridade podem ser desactivados.

Também existe uma relação de dependências de auditoria e disponibilidade com a integridade e confidencialidade, isto é, estes mecanismos garantem a auditoria e a disponibilidade do sistema. Defende ainda o autor que a combinação correcta das características confidencialidade, disponibilidade e integridade facilitam o suporte a organização de forma a atingir os objectivos traçados, dando maior confiança aos seus sistemas de informação. (Idem, 2005)

A autenticidade – é uma outra característica muito importante da segurança de informação que de acordo com Monteiro et al (2000) é o processo através do qual é registado a identidade de um utilizador, dispositivos ou processo. É muito importante para a garantia da segurança

isto porque para garantir a segurança de qualquer outra propriedade primeiramente tem que garantir registo ou seja garantir que a pessoa interveniente é quem afirma que o é.

Não – Repudiação – é outra propriedade de segurança de informação, que proíbe que certo indivíduo rejeita a realização de uma acção. Hoje em dia é uma propriedade muito utilizada em aplicações de comércio electrónico e bancárias. (idem, 2000)

Diz Silva (2004) que a não – repudiação e autenticidade são dois características responsáveis pela verificação da identidade e a autenticidade de uma pessoa externo ao sistema de modo que possam assegurar a integridade de origem.

Por último o **Controlo de Acesso** – que é o processo que limitam ou impedem o acesso não autorizado a certo recurso da organização, encontra-se incluída nesta propriedade funções que limitam a quantidade de recursos a utilizar, o que é de uma forma correcto de ponto de vista da contabilização mas não em relação a segurança. Ainda associado a esta propriedade encontra a função de autorização que estabelecem os direitos de utilizadores, grupos e sistemas. (Monteiro et al, 2000)

Posto isso, a segurança de informação não resume apenas a protecção de informação da organização, mas sim, muito mais do que isso. Diz Carneiro (2002) que *"um dos aspectos mais importante da função segurança, é a subfunção de manutenção e assistência técnica que consistem em:"*

- Conhecer as atribuições e o funcionamento correcto do estabelecimento de trabalho;
- Calendarizar o projecto de revisões do funcionamento do sistema de informação;
- Executar com rapidez e a um custo cada vez mais baixos as tarefas de análise, avaliação e reparação dos serviços;
- Ter capacidade de resposta para que as deficiências ou paragens imprevisíveis sejam corrigidas e ou reduzidas a pouco tempo.

Para finalizar, pode-se dizer que é inquestionável o papel da segurança de informação na organização, a nós, os profissionais desta área é nossa obrigação e responsabilidade pensar a segurança de informação como um todo, propondo ideias e sugestão que possam contribuir para o melhoramento deste processo. Portanto, é importante também compreender a forma como tem sido enquadrado a temática segurança de informação.

2.1 Tipos de segurança de informação

Na abordagem à segurança de informação pode-se encontrar dois tipos: a segurança lógica e a segurança física, que em princípio embora sejam diferentes, complementam-se entre si. Nesta sessão faz-se uma análise profunda da segurança lógica e física, sendo este último com maior destaque. Ver a figura abaixo.

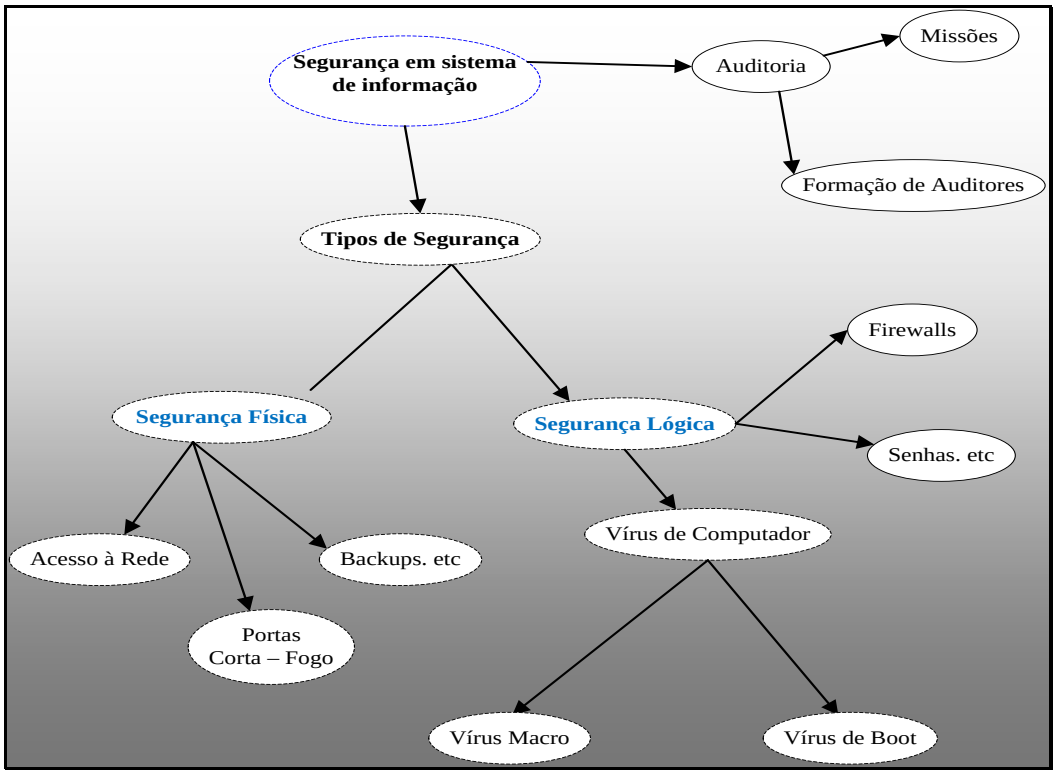

Figura 6 – Tipos da segurança de informação

FONTE: Adaptado de BOGHI & SHITSUKA (2002)

2.1.1 Segurança Lógica

Segundo Clesio (2008) a **Segurança Lógica** – São fronteiras ou barreiras que impedem ou delimitam o acesso a informação, que encontra em espaço controlado, geralmente electrónico, e que, de outro modo, ficaria exposta a modificação não autorizada por elemento mal intencionado. Este mecanismo envolve investimento em *softwares* de segurança ou elaboração dos mesmos.

Esta definição faz um resumo bastante claro daquilo que autor Carneiro (2002) cita na sua abordagem a **segurança lógica** onde diz que este, inclui basicamente três componentes: a segurança de *software*, o controlo de acesso autorizados dos utilizadores e a segurança ou protecção dos dados, dos processos e dos programas.

2.1.2 Segurança Física

Ao contrário da segurança lógica a **segurança física** – é a protecção dos componentes físicos de uma organização. Esta definição é muito restrito, em geral a segurança física permite fazer muito mais do que isso, por exemplo o autor Carneiro (2002) já tem uma definição muito mais ampla que diz que a segurança física não consiste apena na utilização de defesa física e acção de controlo, mas também, na utilização de medida de prevenção contra ameaças aos activos confidencial. Este tipo de segurança diz respeito ao acção de verificação e aos mecanismos de segurança dentro e a volta do centro de processamento de dados (CPD) assim como os meios de acesso remoto implementados para assegurar o *hardware* e os meios de armazenamentos de dados.

Para Grilo & Magalhães (2006) o objectivo fundamental da segurança física consiste na defesa de pessoas bens e instalações das organizações através de implementação de medidas preventivas e/ou reactivas de forma a garantir a continuidade do serviço da organização.

> Segundo Mamede (2006) *"a segurança física é um componente importante de qualquer política da segurança uma vez que, qualquer porta de entrada pode constituir-se como ponto de ataque mais facilmente utilizados. Por isso é extremamente importante que o documento da segurança contém todos os métodos utilizados para a disponibilização e controlo de acesso físicos às*

> *instalações e às condições sob as quais é dado esse acesso. É preciso identificar os métodos de acesso físico, os procedimentos de permissão ou negação de acesso, as restrições, as horas de operação, os pontos de contacto para acesso e os procedimentos para a resposta a incidentes."*

Portanto um documento da segurança física bem desenvolvida, deve abranger os princípios de controlo de acesso, serviços de propagação de incêndios, o abastecimento de energia, o sistema de ar condicionados e a segurança dos recursos humanos, etc. (Carneiro, 2002)

2.1.2.1 Segurança dos recursos humanos ou pessoas

No que diz respeitos à segurança dos recursos humanos ou de pessoas é que no dizer de Promon Business & Technology Review (2005) os recursos humanos ou pessoas são um dos componentes mais importante da segurança de sistemas de informação, isto porque elas são responsáveis por todas as tarefas realizadas na organização começando desde a formação dos profissionais encarregados da segurança até a sensibilização da organização como um todo.

Sendo assim, a política de recursos humanos devem conter um conjunto de aspectos não técnicos relacionados com a admissão e saída do pessoal do quadro dos recursos humanos da organização, a atribuição de níveis de autorização de funcionários e a contemplação de um plano de substituição de ausência com a identificação clara da posição chave na organização. (Mamede, 2006)

Para Grilo & Magalhães (2006) o objectivo da segurança do pessoal é a minimização de risco de falhas humana, roubo, fraude ou mau uso dos recursos da organização. Para isso todos os funcionários devem estar sensibilizados com a política da segurança da empresa. Ela deve englobar os seguintes tópicos:

- A formação dos funcionários sobre as ameaças e outros aspectos da segurança de informação;

- O recrutamento e/ou promoção de empregados idóneos para o cargo relacionado com acesso a informação considerados sensíveis (…);

- A respostas a incidentes, de forma a diminuir os prejuízos causados por falhas da segurança, accionando a aceitação de medidas de correcção adequadas (…).

- Medidas disciplinares para funcionários que transgrediram os procedimentos e as políticas da segurança.

2.1.2.1.1 A formação e sensibilização dos utilizadores

> De acordo com Torres et al (2003) *"uma das formas de ajudar os utilizadores a adoptar a segurança é a sensibilização, que pode ser feita tanto por campanhas de divulgação, como através de sessões de esclarecimentos e formação, mostrando-lhes as razões do que lhes é solicitado e a forma segura de realizar as suas actividades quotidianas como por exemplo, através da aplicação da política de secretaria limpa e da destruição sistemática em equipamento adequado, dos documentos sensíveis, em vez de os deitar no lixo."*

O autor acrescenta ainda que a acção de formação deverá ser preparada em sintonia com a estrutura de recursos humanos e deve abarcar acções que possibilitam os utilizadores competências na realização das tarefas quotidianas de modo a não afectar a segurança de sistema de informação.

No que concerne a campanha de sensibilização refere o autor que este deve compreender questões concretas da segurança abarcando inclusivamente aos aspectos relacionados com *vírus*, *spam* ou questões fundamentais da segurança de organização como por exemplo o mecanismo de autenticação, alertando os utilizadores para as questões do tamanho da *password*, da validação do mesmo, e ainda a importância de escolher ou não *password* do tipo considerado fácil como o caso de data nascimento, e ainda uma outra questão que poderá ser realizado dentro da campanha de sensibilização é a questão de engenheira social. (idem, 2003)

Em suma isto quer dizer que a formação e sensibilização dos utilizadores quando bem desenvolvido e implantada constitui um factor de grande importância para a segurança de informação de qualquer organização.

2.1.2.1.2 O Processo de Recrutamento do pessoal

No que tange ao processo de recrutamento o autor Torres et al (2003) diz que é uma fase muito crítica. Para os autores no caso de um cargo a ser ocupado por um novo pessoal é crítico em relação a segurança de informação a pessoa seleccionada para ocupar este cargo deverá ser informada de todas as regras e princípios da segurança de informação a respeitar na organização. Reforça o autor Mamede (2006) que é preciso disponibilizar informação ao novo funcionário, de modo a lhe permitir a familiarização com as normas e procedimentos estabelecidos pela organização.

Segundo Mamede (2006) o processo de recrutamento do funcionário para uma organização exige um *background*, para que a organização não correr o risco de contratar pessoal com registo criminal informática ou atitudes anormal com a ética informática em outras organizações. O autor defende ainda que quando é recrutado um novo funcionário para a organização deve estar definido o que tem de ser criado a nível de sistema para que este possa ter acesso aos equipamentos informáticos.

2.1.2.2 Segurança dos centros de processamentos de dados e/ou instalação

> *"As instalações constituem o primeiro perímetro físico para a organização, bem como o foco primário da segurança. A infra-estrutura computacional, que inclui os computadores pessoais, servidores, equipamento de rede e demais recursos computacionais utilizados na organização, está localizada no interior das instalações. A política de segurança para as instalações é constituída pelo conjunto de procedimentos e métodos aplicados a esses sistemas e ao ambiente onde operam."* (Mamede, 2006)

Segundo Torres et al (2003) a localização do centro de dados consiste na descrição de um conjunto de orientações que permite a localização e a configuração correcta dos centros de dados. Para o autor este deve respeitar as seguintes regras:

- Nunca deve ficar situado nos rés de chão nem no último piso do edifício;

- Se no caso do edifício é constituído por únicos rés de chão o centro de dados deverá ficar situado no local mais escondido dos lugares da circulação pública;

- Não deve existir qualquer acesso directo de lado de fora às salas de centro de dados como por exemplo janelas, portas respiratórios, etc.

- Não deve existir qualquer conduta de águas ou de esgotos próximo dos centros de dados;

- O lugar onde fica os centros de dados deve ser dotados de tecto falso para a passagem de serviços de alimentação aos centros de dados.

2.1.2.3 Segurança dos equipamentos

Grilo & Magalhães (2006) defende que a segurança dos equipamentos consiste na tomada de medidas de segurança que permite o impedimento de perda, dano ou prejuízo de equipamentos informáticas ou a suspensão de serviços da organização. Para a segurança dos equipamentos são fundamentais as medidas tais como:

- Instalações de UTS *(uninterruptable power suply*) ou geradores de emergência para protecção dos equipamentos contra falhas;

- Manutenção correcta dos equipamentos respeitando a especificação do fabricante de forma a garantir a integridade e disponibilidade do mesmo;

- Eliminação ou cifragem de informação considerado sensível sempre que for necessário a reparação de equipamentos;

- Utilização de cadeados, cabos para prevenir contra roubos da estação de trabalhos;

- Destruição de suportes removíveis, com informação sensível sempre que estiverem danificados, etc.

> Segundo Silva (2005) *"a segurança do equipamento impede a perda, dano e acesso não autorizados aos equipamentos duma organização, implementando medidas de segurança desde a sua instalação, manutenção até a sua destruição. A segurança do equipamento, deve impedir acessos não autorizados mas, nunca deve por em causa a disponibilidade e a integridade do mesmo."*

3 Análise de riscos em sistema de informação

Provavelmente pode-se dizer, que o mundo de hoje caminha para uma sociedade de informação, e a consequência disso será o aumento da utilização dos sistemas de informação na organização que, por conseguinte, também aumenta a probabilidade de ocorrência dos riscos, e das ameaças aos sistemas de informação. Neste contexto todas as organizações querem estar protegidos das ameaças e riscos que possam causar problemas aos seus sistemas de informação.

Para Carneiro (2002) a principal causa da insegurança de um sistema deve-se por três motivos:

- Desconhecimentos técnicos dos procedimentos fundamentais que garante a segurança de sistema por partes das pessoas;

- A negligência dos utilizadores;

- A não formulação e nem adaptação de uma política de segurança para a organização por partes das decisores das vários áreas estratégicos da organização.

Para melhor compreender a temática análise de risco definiu-se algum conceito considerado importante para a compreensão do mesmo.

Segundo Zúquete (2006) uma **vulnerabilidad**e é uma falha no sistema que dá o atacante a possibilidade de fazer ataque ao sistema, um **ataque** é um conjunto de procedimentos executados por um atacante no âmbito de explorar a vulnerabilidade de sistema, enquanto

riscos são danos provocados por realização de ataques ao sistema. A figura abaixo faz um resume bastante clara da relação existente entre os principais conceitos.

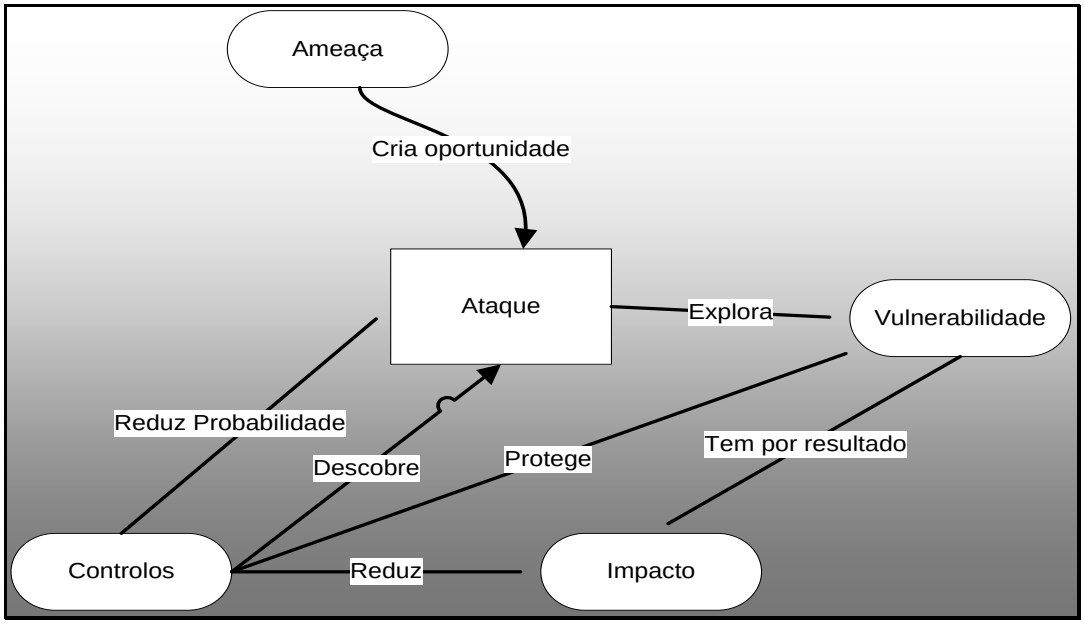

Figura 7 – Componentes de análises de riscos

FONTE: adaptado de MAMEDE (2006)

Também pensa-se pertinente conhecer os diferentes tipos de risco que possam afectar o sistema de informação de uma organização.

3.1 Tipos de riscos

De acordo com Zúquete (2006) os riscos aqui mencionados são relativamente aos computadores. Como foi referido no primeiro capítulo o computador é um dos elementos integrante dos sistemas de informação por isso pensa-se importante abordar os seguintes tipos de riscos:

- **Intrusões –** são alteração comportamental de uma máquina ou aplicações provocados por um ataque. Este tipo de risco é de difícil avaliar porque não implica qualquer dano objectivo, mas garante os intrusos capacidade que lhe são rejeitados de impor danos maiores usando para esse efeito a máquina invadido.

- **Acesso a informação reservada ou confidencial** – como sabe-se a função de computador não é somente processar informação, mas também, o armazenamento de informação cujo acesso deverá ser controlado, sendo assim qualquer acesso não autorizado constitui riscos para o dono da informação.

- **Perda ou roubo de informação ou equipamentos** – a perda ou roubo de informação armazenado num dispositivo ou computador faz com que perdemos como é óbvio a informação considerados confidenciais para a posse de quem roubou a informação ou dispositivos de informação, sendo assim constituir um risco para a organização.

- **Personificação** – este tipo de risco acontece sobretudo quando uma máquina é usada por mais de um utilizador que é distinguido e autenticado pelo sistema, e este destrói, os sistemas de autenticação do outro fazendo passar por outro para realizar actividades nessa máquina. Ela é usada para dois efeitos: para o despiste quando se pretende que a verdadeira identidade da máquina usada num ataque seja escondida, o que é normalmente útil em *ataques DoS,* também utiliza-se apropriação para a utilização de uma identidade indiferente, que serve para ultrapassar barreira de segurança, como barreiras simples de autenticação e autorização baseado em identidade.

- **Incapacidade de prestação de serviço** – através de um ataque *DoS* a máquina ou dispositivos pode ficar impossibilitado de prestar serviços, e consequentemente ocorre a falha ou risco na prestação de serviços. Neste tipo de risco quanto mais importante for a relevância da máquina para os utilizadores ou para os componentes de sistema distribuído aqui pertence maior será o risco.

Em suma conclui-se que é muito importante que toda e qualquer área da organização tenham profissionais com capacidade de entender a natureza e a probabilidade dos risco, saber qual é a consequência de inexistência da segurança e ainda conhecer os possíveis vulnerabilidades e as diferentes soluções para a organização. (Carneiro, 2002)

Após conhecer os possíveis riscos que possam afectar o sistema de informação de uma organização, importa agora conhecer quais são as etapas de análise do mesmo. A sessão que se avizinha aborda de forma profunda os principais etapas de análise de risco.

3.2 Etapas de análise de risco

Segundo Monteiro (2009) o processo de análise de risco são utilizados pela organização para identificar o nível de risco e ameaças que envolvem os sistemas de informação. Neste contexto após identificação dos riscos que envolvem os sistemas de informação cabe a organização decidir o que fazer em detrimentos dos riscos identificados. É da responsabilidade da organização eliminá-los, minimizá-los, compartilhá-los ou assumi-los.

Na perspectiva de Monteiro et al (2000) o principal objectivo da análise de risco é a identificação dos activos a proteger, a identificação dos ameaças e a determinação dos custos de protecção e da recuperação de um ataque.

Reforça ainda o autor que "*ela deverá tentar quantificar a probabilidade de sucesso de uma tentativa de ataque, avaliando os acessos ao exterior existente, o mecanismo de autenticação em utilização, os mecanismos/sistemas de firewall existentes e ainda, os potenciais ganhos de um atacante."* (Idem, 2000)

Deste modo reconhecendo a importância da análise de risco para qualquer organização, então pode-se dizer que as etapas de análises de riscos permitem eliminar ou minimizar os pontos de ataques e as vulnerabilidades explorados por atacantes numa organização. Segundo Grilo & Magalhães (2006) as etapas fundamentais de análise de risco são:

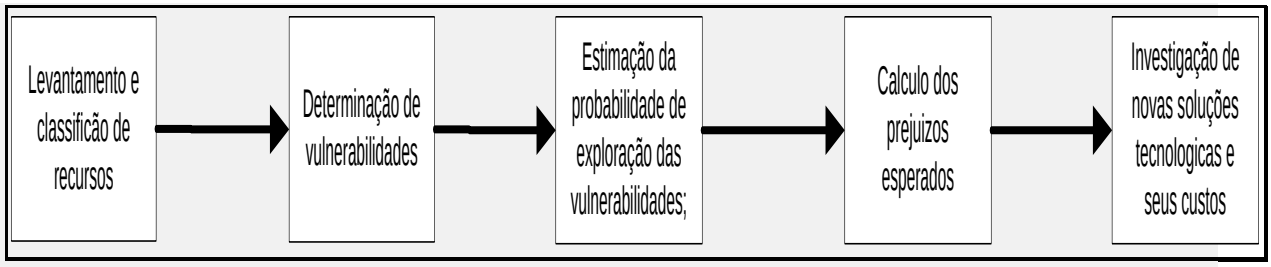

Figura 8 – Etapas de análise de risco

- **Levantamento e classificação de recursos** – é a primeira etapa de análise de risco, que consiste em fazer a recolha e classificação dos recursos humanos e materiais da

organização, ou seja, consiste em proceder um inventário correcto dos recursos necessários para organização.

- **Determinação da vulnerabilidades –** Este constitui a segunda etapa e é bem mais difícil que a primeira, isto porque, consistem em determinar as vulnerabilidades dos recursos existentes. Para a determinação da vulnerabilidade o autor considera que é importante levar em conta algumas questões e cenários que possam surgir tais como: Quais são os efeitos provocados por erros não intencional? Quais são efeitos provocados por actos interno e/ou externo malicioso? Quais são os efeitos provocados por acções catástrofes físicas e naturais?

- **Estimação da probabilidade de exploração das vulnerabilidades –** É a terceira etapa de análise de risco que consiste em determinar o grau de frequência de cada vulnerabilidade ser explorada. A probabilidade de ocorrer ou não, uma eventual ataque depende do nível da segurança da própria organização com a probabilidade de alguém derrubar essa segurança. Diz ainda o autor que mesmo ser impossível prever a probabilidade de ocorrência de eventos existem mecanismo que possibilita estimar essa probabilidade como por exemplo, a observação de dados da população em geral; a observação de dados locais; através do número de casos registados num determinado período do tempo e o método de Delphi.[3]

- **Cálculo dos prejuízos esperados –** a quarta etapa consiste em calcular de forma clara os custos em relação a componentes de *hardware e software* ou aplicações das organizações. Este cálculos deverá ser pensados com bases nos eventuais constrangimentos das actividades da organização como por exemplo falhas de uma aplicação ou de um componente de *hardware*.

[3]"**Método de Delphi** – é uma técnica em que diversos analistas estimam individualmente a probabilidade de ocorrência de um evento. As estimativas são depois reunidas, reproduzidas e distribuídas a todos os analistas. De seguida, é feita a pergunta aos analistas se desejam modificar algumas das probabilidades estimadas com base nas fornecidas pelos colegas. Após um conjunto de revisões, todas as estimativas são novamente reunidas. Se os valores forem razoavelmente consistentes, a estimativa final é inferida. Se forem inconsistentes, os analistas reúnem-se novamente para discutir a razão da incoerência e seleccionarem uma estimativa final." (Grilo & Magalhães, 2006)

- **Investigação de novas soluções tecnológicas e seus custos** – É a última etapa que consiste na instalação de novas soluções tecnológicas a nível de segurança oferecido e a nível de custo de aquisição e instalações dos equipamentos. [4]

De modo geral, afirma Mamede (2006) que a análise de risco permite fazer uma aproximação consistente e objectiva às questões da segurança de forma horizontal a toda organização e sistema, abrangendo os sistemas informática e todos aqueles que não estão sob controlo do departamento tecnológica.

3.3 Sistema de gestão da segurança de informação

Segundo ISO/IEC 17799 (s/d) apud Promon Business & Technology Review (2005) o sistema de gestão da segurança de informação (**SGSI**) é (…), um instrumento de gestão que incorpora a definição de estrutura da organização, definição de papéis, política da segurança da organização e a gestão baseada na gestão de risco para implementar, operar e monitorar de forma proactiva a segurança de informação.

De acordo com Promon Business & Technology Review (2005) este sistema não resolve na totalidade os problemas da segurança mas trata de sistematizar a gestão de risco e descrever as melhores práticas para tratá-los. Um documento de SGSI deve abarcar três elementos da segurança de informação, as políticas, os processos e os procedimentos da segurança de informação.

Porém ainda de acordo com ISSO/IEC 17799 (s/d) apud Promon Business & Technology Review (2005) a implantação do sistema de gestão da segurança de informação deve ser semelhante a dos sistemas de gestão da qualidade e meio ambiente abarcando o ciclo de PDCA (*Plan – Do – Check – Act*) que significa em português planear, executar, verificar e agir.

[4] Baseado nos autores Grilo, Alberto & Magalhães Hugo. (2006) *A segurança informática e o negócio electrónico.* [em linha], disponível em <http://www.spi.pt/negocio_electronico/documentos/manuais_PDF/Manual_VII.pdf>, [consultado em 12-05-2010].

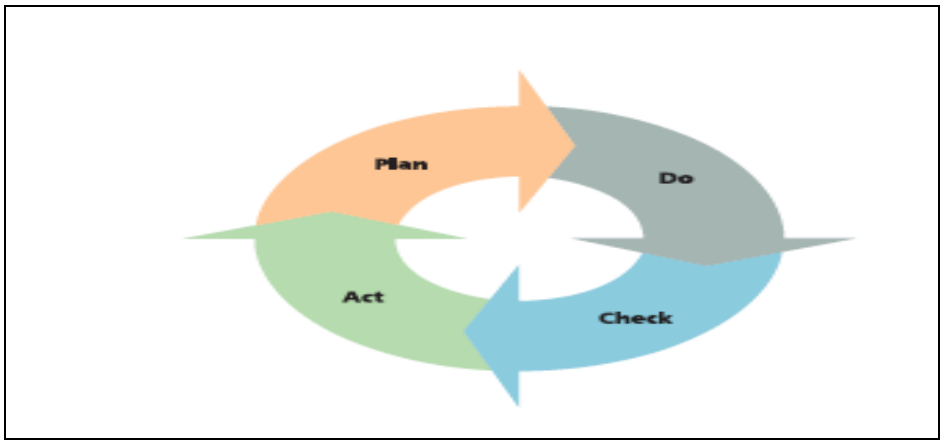

Figura 9 – Ciclos do sistema de gestão de segurança de informação

FONTE: PROMON, Business & TECHNOLOGY Review (2005)

- **Plan** – Ciclo que permite delinear um conjunto de orientações para estabelecer a segurança de informação de acordo com os objectivos do negócio de uma organização. Permite ainda fazer descrição geral dos activos de informação da organização e a atribuição de valores para cada activo, conhecer suas vulnerabilidades, ameaças e o impacto agregados a cada ameaça.

- **Do** – Este ciclo permite definir planos para o tratamentos de questões de riscos tais como risco que afecta a instalação de ferramentas os processos de formação a sensibilização a criação de regras de trabalhos e ou transferir o risco ao terceiro.

- **Check –** Esta fase é responsável pelos serviços de monitorização e verificação do SGSI, ou seja, averigua, se em relação aos riscos identificados, os planos traçados foram apropriados e se o sistema atingiram os objectivos traçados.

- **Act –** É a fase responsável pela permanência do sistema de gestão da segurança de informação de acordo com os objectivos da organização. Permite verificar se a adequação do SGSI está de acordo com os objectivos iniciais e novas da segurança da organização e apontar soluções de melhorias do sistema.

Em geral, afirma Promon Business & Technology Review (2005) que estas normas devem ser aplicadas em qualquer processo ou sector de uma organização e que a melhor seria aplicada num âmbito mais restrito da organização e com o passar de tempo ampliar este processo por toda outras áreas da organização.

4 Políticas da segurança de informação

Partindo da perspectiva que a informação e sistema de informação são componentes indissociáveis para qualquer organização, então alguma política da segurança deve ser implantada de forma a assegurar o funcionamento do mesmo.

De acordo com Ed. Titel (2003) não existem uma única política da segurança para todos os sistemas de informações, mas existem alguns pontos em comum que devem ser importante para qualquer organização.

Diz Freitas & Lauro (s/d) que numa política de segurança de informação os pontos em comum que podem ser utilizados em qualquer organização abarcam os seguintes tópicos:

- Declaração do comprometimento da alta administração com a PSI, apoiando suas metas e princípios;
- Objectivos da segurança da organização;
- Definição de responsabilidades gerais na gestão da segurança de informações;
- Orientações sobre análise e gestão de riscos;
- Princípios de conformidade dos sistemas computacionais com a PSI;
- Padrões de controlo de acesso a recurso e sistemas computacionais;

- Classificação de informações (de uso irrestrito, interno, confidenciais e secretas);

- Procedimentos de prevenção e detecção de vírus;

- Princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, directos sobre software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);

- Princípios de supervisão constante das tentativas de violação da segurança de informações;

- Consequências de violações de normas estabelecidas na política de segurança;

- Princípios de gestão da continuidade do negócio;

- Plano de formação em segurança de informações.

De acordo com Spanceski (2004) a PSI é o alicerce de todos os problemas relacionados com à protecção de informação, desempenhando uma função crucial para qualquer organização, isto porque delineia normas, procedimentos, ferramentas e responsabilidades para sustentar o controlo e a segurança de informação de qualquer organização.

Na perspectiva de Grilo & Magalhães (2006) as políticas da segurança são procedimentos normas e regras que permitem controlar a informação confidencial, aplicação/programa, dispositivos físicos ou instalação numa organização.

Também no entender de Moraes & Cirone (2003) as políticas da segurança são conjuntos de regras, procedimentos, autorizações e negação que garantem a manutenção da segurança e da confiabilidade da rede.

> Para Freitas & Lauro (s/d) *"a política de segurança de informações deve conter princípios, directrizes e regras genéricos e amplos, para aplicação em*

> *toda a organização. Além disso, ela deve ser clara o suficiente para ser bem compreendida pelo leitor em foco, aplicável e de fácil aceitação. A complexidade e extensão exageradas da PSI podem levar ao fracasso da sua implementação. Cabe destacar que a PSI pode ser composta por várias políticas inter-relacionadas, como a política de senhas, de backup, de contratação e instalação de equipamentos e softwares."*

Afirma Dias (2000) apud Laureano (2005) que a PSI deve abarcar para além de componentes relacionados com sistemas de informação, mas também, deve abarcar aspectos relacionado com a política institucional da organização, objectivos de negócios e planeamento estratégico da organização.

No mesmo ponto de vista defende Freitas & Lauro (s/d) que uma política da segurança de informação (PSI) não deve abarcar apenas a área informática mais sim deve abranger todo o sistema de informação e recursos computacionais de uma organização ou seja ela deve integrar à visão, a missão, ao negócio e às metas organizacionais, bem como ao plano estratégico de informática e às políticas da organização respeitante à segurança no seu todo conforme ilustra a figura abaixo:

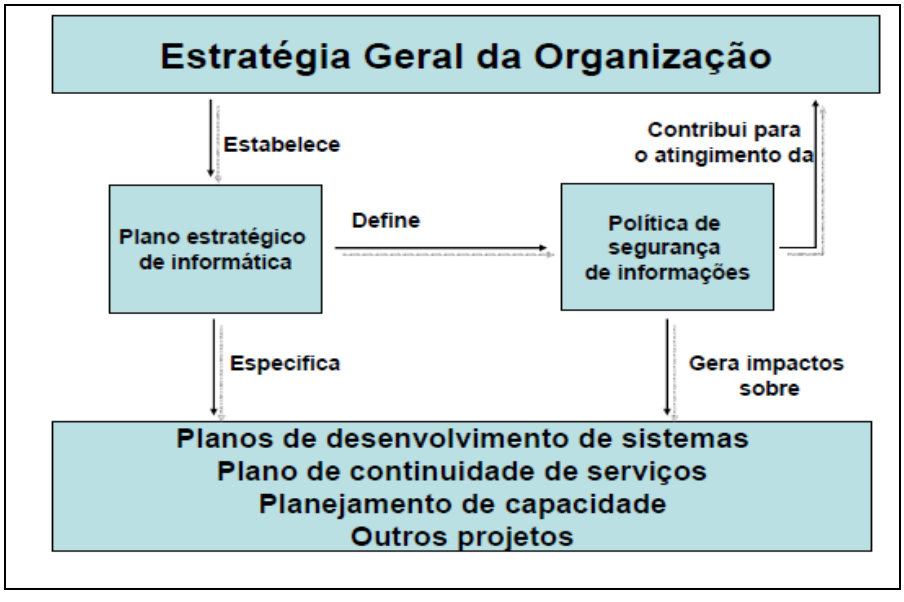

Figura 10 – Aspecto da PSI de uma organização

FONTE: LAUREANO, P. A. Marcos (2005)

Pode-se dizer então que uma PSI é um documento formal escrita e divulgada por uma organização com objectivo de regulamentar o funcionamento do mesmo. Porém ela deve ser um documento simples e objectivas que abrange todos os activos da organização, possibilitando uma compreensão rápida por parte dos colaboradores de sistema de informação da organização.

De acordo com Freitas & Lauro (s/d) é aconselhável que numa organização existe um departamento encarregado pela segurança de informações, que inicia o processo de criação de política da segurança de informação, bem como coordenar sua implantação, aprová-la e revisá-la, além de designar funções da segurança. Também é importante que as pessoas da área crítica da organização sejam elementos participativos do processo de elaboração da PSI, (…).

4.1 Política de *Password*

Segundo Cima F. (s/d) é importante ter em mente que uma política de senhas é um controlo da segurança e antes de definir uma política de senha devemos compreender os riscos que queremos evitar que dependem inclusivamente do valor do que está sendo protegido com a senha, e dos outros controlos de acesso que existem adicionalmente além da própria senha. Também é importante compreender contra o quê estamos nos protegendo ao aplicar uma política de senhas.

> De acordo com Fauri (2009) *"a mudança periódica de senhas é uma prática que deveria ser considerada uma rotina por todos os utilizadores, em especial pelos internautas. Em tempos onde o roubo de informações é o principal objetivo de ameaças digitais, a adoção de alguns conceitos relacionados à segurança de dados é crucial. Infelizmente, as pessoas geralmente esperam o pior acontecer, para então tomar medidas que deveriam ser consideradas corriqueiras; a adoção de simples normas em seu dia a dia fará com que tenha menos problemas relacionados ao roubo de senhas."*

Sendo assim é importante considerar aqui um conjuntos de normas e regras que devem ser definida e respeitada universalmente por toda organização no uso da política de senha. De

acordo com os autores Cima F. (s/d) & Fauri (2009) uma política de senha segura deve respeitar os seguintes regras:

- Exigir tamanho mínimo e complexidade do *password*, com a mistura de letras, números, simbolos, maiúsculas e minúsculas de forma a evitar ataques de força bruta ou dicionários;

- Fazer a troca periódicamente da política de senha pelomenos num prazo de três a quatro meses;

- Bloquer a conta do utilizador após vários tentativas de autenticação realizado de forma incorrectas de modo a proteger contra ataques de força bruta e dicionário;

- Memorizar a sua senha em vez de o guardar em qualquer lugar, e evitar memorizar senhas oforecidas por vários *sites* e *softwares* ou então fazer o uso desse recurso somente em seu próprio computador;

- Evitar o uso da mesma senha para todos os registos realizado na internet.

Em nota de resumo, afirma Mamede (2006) que o *password* como um elemento importante de identificação de utilizadores deve ser criado, gerido e definida de forma clara, especificando as etapas a seguir e as autorizações necessárias para a criação do perfil de utilizador com a respectiva senha. Ainda deve estar indicado um conjunto de recumendações aos utilizadores tais como: quais os mecanismos de auditoria a implementar, como escolher uma senha e prazos de validade do mesmo.

4.2 Política de *E-mail*

De acordo com Bastos (2005) pode-se dizer que hoje em dia grande parte da comunicação é feita através de *e-mail* mas também grande parte dos vírus electrónicas actuais são enviadas por esse meio, por isso é importante conhecer algumas regras e normas que devem ser assimilada por toda a organização na utilização desse importante meio de comunicação.

Diz ainda Bastos (2005) & Mamede (2006) que existem um conjunto de regras e procedimentos que devem ser seguida numa organização na política de uso de *e-mail*. De entre elas destacam-se os seguintes:

- Não abrir anexos com extensões, .Bat, .Exe, Src, .Link e .Com se não tiver certeza absoluta de quem solicitou esse *e-mail*;

- Desconfiar de todos os *e-mails* com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como ILOVEYOU, BRANCA DE NEVES, etc;

- Não reenviar *e-mails* do tipo corrente, como por exemplo aviso de *vírus*, avisos de *Microsoft/AOL/Symantec*, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc;

- Não utilizar o *e-mail* da empresa para assuntos pessoais, e nem mande *e-mails* para mais de dez pessoas de uma única vez (to, cc, bcc);

- Utilizar sempre sua assinatura criptográfica para a troca interna de *e-mails* e quando necessário para os *e-mails* externo;

- Devem-se alertar os utilizadores para o risco de enviar informação confidencial do negócio em mensagens de correio electrónico (*e-mail*) que podem constituir um perigo para a comunicação;

- A dimensão dos anexos das mensagens a enviar deve ter um tamanho máximo definido, de modo a não haver problemas de negação de serviço, de forma inadvertida, (…).

- Devem ser declarada que o *e-mail* não pode ser utilizado para fins ilegais ou incorrectos, que transgride os direitos de qualquer tipo de propriedade, (…).

4.3 Política de acesso a Internet

A Internet é hoje em dia uma das ferramentas mais poderosa do trabalho, por isso ela deve ser acessado e usado de forma restrita, respeitando os seguintes tópicos: (Bastos, 2005)

- Permitido somente para a navegação de *site*. Em relação aos casos específicos que exijam outros protocolos deverão ser solicitados directamente a equipa da segurança com prévia autorização do responsável do departamento local;

- Bloquear e monitorar o acesso aos *sites* com conteúdo perniciosos, jogos, bate-papo, apostas e assemelhados;

- Proibir o uso de ferramentas P2P (*Kazaa, Morpheus*, etc.);

- Proibir o uso de IM (*Instant messengers*) não homologados e autorizados pela equipa da segurança;

4.4 Política de uso de Estação de trabalho

Neste caso referiu-se a estação de trabalho como sendo qualquer computador ligado a rede. Portanto diz Bastos (2005) que cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede, e cada pessoa possui sua própria estação de trabalho. Isto significa que tudo que foi feito ou venha ser feito na sua estação de trabalho é da sua responsabilidade, por isso sempre que sair do seu local de trabalho efectua *logoff* ou trava o console. As principais regras que devem ser respeitadas na política de uso de estação de trabalho são as seguintes:

- Proibir a instalação de qualquer tipo de *software* e ou *hardware* sem a ordem da responsável técnico da segurança da organização;

- Proibir a utilização de MP3, filmes, fotos e *softwares* com direitos autorais ou qualquer outro tipo de pirataria;

- Guarda na sua estação de trabalho somente coisas supérfluo ou pessoal, e os restantes dados ou informação da organização devem ser guardado no servidor onde existem um sistema de *backup* diário e confiável. Caso não sabe como fazer pergunta o responsável técnico da segurança da organização.

5 Planeamento da segurança de informação

Segundo Torres et al (2003) *"num programa transversal a toda empresa, como o caso do programa de segurança, o planeamento é fundamental para conseguirmos, no final, avaliar a eficácia das medidas tomadas."*

Contudo é importante que um plano seja flexível e independente, porque um plano que é difícil de alterar, ou seja com uma lógica particular e elementos muito específico poderá dificultar mais do que ajudar numa situação de desastre. (Idem, 2003)

No entender de Ferreira (1995) o método de planeamento da segurança consiste em garantir que as actividades críticas da organização sejam restabelecidas e mantidas a mais rápida possível após a ocorrência de uma falha ou desastre, e ela deve recair sobre a manutenção de tarefas críticas e serviços em execução, abarcando o pessoal e outros recursos não computacionais e deverá incluir as seguintes aspectos:

- Identificação e priorização das actividades críticas;
- Avaliação do impacto potencial dos vários tipos de acidentes (desastres) nas actividades da organização;
- Identificação e aprovação de todas as responsabilidades e medidas de emergência;
- Documentação dos métodos e processos aprovados;
- Formação do pessoal;

- Teste dos planos;

- Actualização dos planos.

5.1 Tipos de planos

No ponto de vista do mesmo autor existem três tipos de plano da segurança de informação (Contingência, Reposição e Recuperação) e cada plano da segurança deverá ter diferentes níveis, isto porque, cada nível terá incidências diferentes e poderá envolver diferentes equipas de recuperação.

5.1.1 Plano de contingência

> Freitas & Lauro (s/d) diz que *"Actualmente, é inquestionável a dependência das organizações aos computadores, sejam eles de pequeno, médio ou grande porte. Essa característica quase generalizada, por si só, já é capaz de explicar a importância do Plano de Contingências, pois se para fins de manutenção de seus serviços, as organizações dependem de computadores e de informações armazenadas em meio electrónico, o que fazer na ocorrência de situações inesperadas que comprometam o processamento ou disponibilidade desses computadores ou informações? Ao contrário do que ocorria antigamente, os funcionários não mais detêm o conhecimento integral, assim como a habilidade para consecução dos processos organizacionais, pois eles são, muitas vezes, executados de forma transparente. Além disso, as informações não mais se restringem ao papel, ao contrário, elas estão estrategicamente organizadas em arquivos magnéticos.*"

Neste âmbito defende Pinheiro (2007) que o objectivo principal de um plano de contingência é tomar medidas imediata recorrendo aos procedimentos de recuperação dos sistemas corporativos, levando em conta o tempo de espera previsto para o restabelecimento da actividade definido pelos gestores do sistema, (…).

Segundo Torres et al (2003) o plano de contingência são constituídos por planos que encontram delineado as respostas iniciais a um incidente por parte de todas áreas que compõem uma organização, quer este ocorra com ou sem aviso prévio, ela abrange todas os procedimentos de emergência, descrição das equipas que executam, informação facilitadora da execução e indicação dos eventos que despoletam os procedimentos.

Segundo Laureano (2005) & pinheiro (2007) o plano de contingência encontra-se subdividido em três planos (planos de administração de crise, plano de continuidade operacional e plano de recuperação de desastre) que complementam entre si:

5.1.1.1 Plano da Administração de Crise

Segundo Laureano (2005) este plano delineia fases por fases o funcionamentos das equipas que abrange o accionamentos da contingência antes, durante e depois da ocorrência do acontecimento e ainda define os procedimentos a serem tomados pela mesma equipa no período de retorno à normalidade.

5.1.1.2 Plano de Continuidade Operacional

Ao contrário do plano de administração de crise também o plano de continuidade operacional é um documento que definem os procedimentos para contingência dos activos que suportam cada processo de negócio, objectivando reduzir o tempo de indisponibilidade e consequentemente, os impactos potenciais ao negócio. Permite orientar as acções diante da queda de uma conexão à Internet, exemplifiquem os desafios organizados pelo plano. (Idem, 2005)

5.1.1.3 Plano de Recuperação de Desastres

Para Aurelio (2005) Este plano consiste em minimizar a probabilidade de ocorrência de interrupção e repor o funcionamento da organização. Ainda defende o autor que este plano trata o porquê, o quê, quem, onde, e quando da recuperação de actividade e procedimento de negócio da organização.

Na perspectiva de Ferreira (1995) plano da recuperação trata de criar cópias de segurança (*backup*) de toda a informação considerada importante do sistema. Ela deve abranger a periodicidade das cópias da segurança, números de exemplares das cópias da segurança, localização do arquivo de suportes magnéticos e procedimentos de reposição.

Defende Torres et al (2003) que o plano de recuperação a semelhança do plano de contingência para além de incluir procedimentos para cada processo e actividade críticos, ela deverá incluir a estrutura e constituição das equipas que executam plano de acção e todas as informação disponibilizada que tornará mais fácil implementar os procedimentos de sistemas, dados, comunicação de dados voz, posto de trabalho e processos tecnológico e não tecnológico.

Desta forma pode-se dizer que os respectivos planos da segurança supra-citado tem como objectivos minimizar e garantir o normal funcionamento da organização faces aos desastres ocorridos antes e depois de acontecimento numa organização.

Capítulo 3: A Segurança em sistema de informação governamental

1 Enquadramento

Neste capítulo apresenta-se a segurança em sistema de informação governamental, onde debruça-se sobre conceito de governo, sistemas de informação governamental, neste último destacando os diferentes tipos dos sistemas de informação governamental existentes.

De seguida fala-se da segurança dos sistemas de informação governamental de uma forma geral e por último particularizando-o à realidade Cabo-verdiana.

2 Conceito do governo

Segundo a Constituição da República de Cabo Verde (art.185) governos são órgãos superiores administrativos públicos cuja função é definir, dirigir e executar a política geral interna e externa do país.

Normalmente um governo encontra-se estruturado por órgãos representativos do povo, formado por um Primeiro-ministro, Ministros e Secretário de Estado. (CRCV, art.186)

De acordo com Varican (1999) governos são grupos de organização, instituição e liderança responsáveis pela administração pública e pela direcção dos Estados. Ele pode ser classificado

quanto ao regime de governo podendo ser governo de República e Monarquia, quanto à forma de governo podendo ser Parlamentarismo, Presidencialismo e Formas mista de governo e também quanto aos regimes políticos como governo Democrático e Ditatoriais.

O papel do governo é prestar serviços aos cidadãos. O processo de administração pública consiste no processamento de dados/informação. A função do governo é colectar e processar dados e informações sobre os indivíduos, famílias, organizações e empresa, que de seguida, apoiados nos dados e informação recolhida, produzem novas informações para o público, tais como, políticas, estratégias, planos, regulamentos e diversos serviços ao público. As tecnologias de informações são utilizadas para suportar o processamento de informações dos governos, incluindo a recolha de dados, armazenamento, processamento, disseminação e utilização. (Nações Unidas, 1995)

3 Sistemas de informação governamental

Segundo Favero et al (2006) devido ao melhoramento de comunicação acompanhado da dinâmica das ferramentas tecnológicas, pode-se entender que os sistemas de informação são importantes para organizações públicas porque possuem elementos que facilitam o controlo e a prestação de contas dos resultados do mesmo com a sociedade.

Para os mesmos autores o motivo da utilização dos sistemas de informação na administração pública como forma de viabilizar o controlo e garantir mais segurança e transparência é justificado pela modernização, pela melhoria na gestão administrativa, financeira, tributária e patrimonial, (…).

De acordo com as Nações Unidas (1995) os governos são os maiores utilizadores de TI. E normalmente as TI são utilizadas nas áreas de tributações, gestão financeira, estatística, segurança social, ordenamento do território, agricultura e outras áreas como a de polícia, defesa e segurança nacional e investigação etc.

3.1 Tipos dos sistemas de informação governamental

Tal como outras organizações, o governo também pode ser estruturada em três níveis: ao nível estratégico, ao nível administrativo ou de gestão (táctico) e ao nível operacional onde cada um destes níveis representa um nível diferente de controlo. (Idem, 1995)

Para as Nações Unidas (1995) atendendo aos três níveis das organizações, acima mencionados, os sistemas de informação governamental podem ser divididos em três tipos de sistemas, fazendo parte destes, os operacionais, de informação de gestão e os de apoio a tomada de decisão, (Ver capítulo 1, que explica de forma clara os diferentes tipos de sistemas de informação). Também refere ainda o autor que existe mais dois tipos de sistemas de informação que também são de grande importância para a administração pública:

- **O sistema de gestão e recuperação de documentos** (DMRS) **–** Sistemas com o objectivo de manipular dados entre o governo, apoiar texto, forma de imagem, dados de áudio e vídeo em tempo real. Também este sistema fornece os utilizadores muito mais flexibilidade do que a base de dados para organizar e visualizar os dados críticos. O que diferencia DMRS (Sistemas de gestão e recuperação de documentos) do SGBD (Sistemas de gestão de bases de dados) é a sua capacidade de gerir informação semi-estruturados ou não, como por exemplo o texto em execução em um arquivo de texto ou os padrões de *(bit-mapped)* em um fax ou desenho digitalizado, ou seja este sistema tem o potencial para gerir grande maioria das informações tratadas por qualquer organização.

- **O sistema de informação geográfica** (SIG) – Sistemas que analisam o contexto geográfico das organizações, bem como o relacionamentos entre elas, oferecendo a possibilidade de visualizar eventos a nível detalhado. Também ajuda a mente humana a assimilar e compreender a informação, permite o utilizador tomar decisões baseado no contexto espacial correcto. Estes sistemas são cada vez mais utilizados na administração pública para fins diferentes daquele que englobam a topografia tradicional e gestão imobiliária. Sua aplicação é cada vez mais comum em sectores como avaliação do impacto ambiental, ordenamento do território, gestão de recursos, planeamentos urbano/regional, (…) etc.

3.2 Segurança em sistemas de informação governamental

Segundo Lima et al (2000) é essencial garantir o direito dos cidadãos à privacidade, o direito à consulta dos dados colectados nos sistemas governamentais de acordo com a constituição. Os *Websites* públicos devem responsabilizar pela garantia da confidencialidade das informações de carácter pessoal que são depositadas em suas bases de dados, sejam elas referentes aos utilizadores ou pessoas que fazem parte da administração pública.

Para os mesmos autores é importante identificar o motivo relacionado com as vulnerabilidades do tratamento da informação, da compreensão dos diversos ambientes do contexto governamental e da aceitação de um modelo da segurança que minimiza os vários efeitos das vulnerabilidades.

> *"A modelagem da segurança, nas suas diversas formas, é um dos componentes que influi na credibilidade de um sistema de computadores, conectado ou não em rede. Esta, sob um contexto mais amplo, propõe um maior controlo sobre os activos de informação, assim como sobre os serviços disponibilizados pelas diversas áreas do Governo. Torna mais tangível a avaliação da qualidade dos serviços e a responsabilização sobre o uso indevido ou a má administração de tais recursos."* (Lima et al 2000)

O modelo de segurança de informação (MSI) nas instituições públicas deve guiar para os seguintes detalhes conforme ilustra a figura abaixo. (idem, 2000)

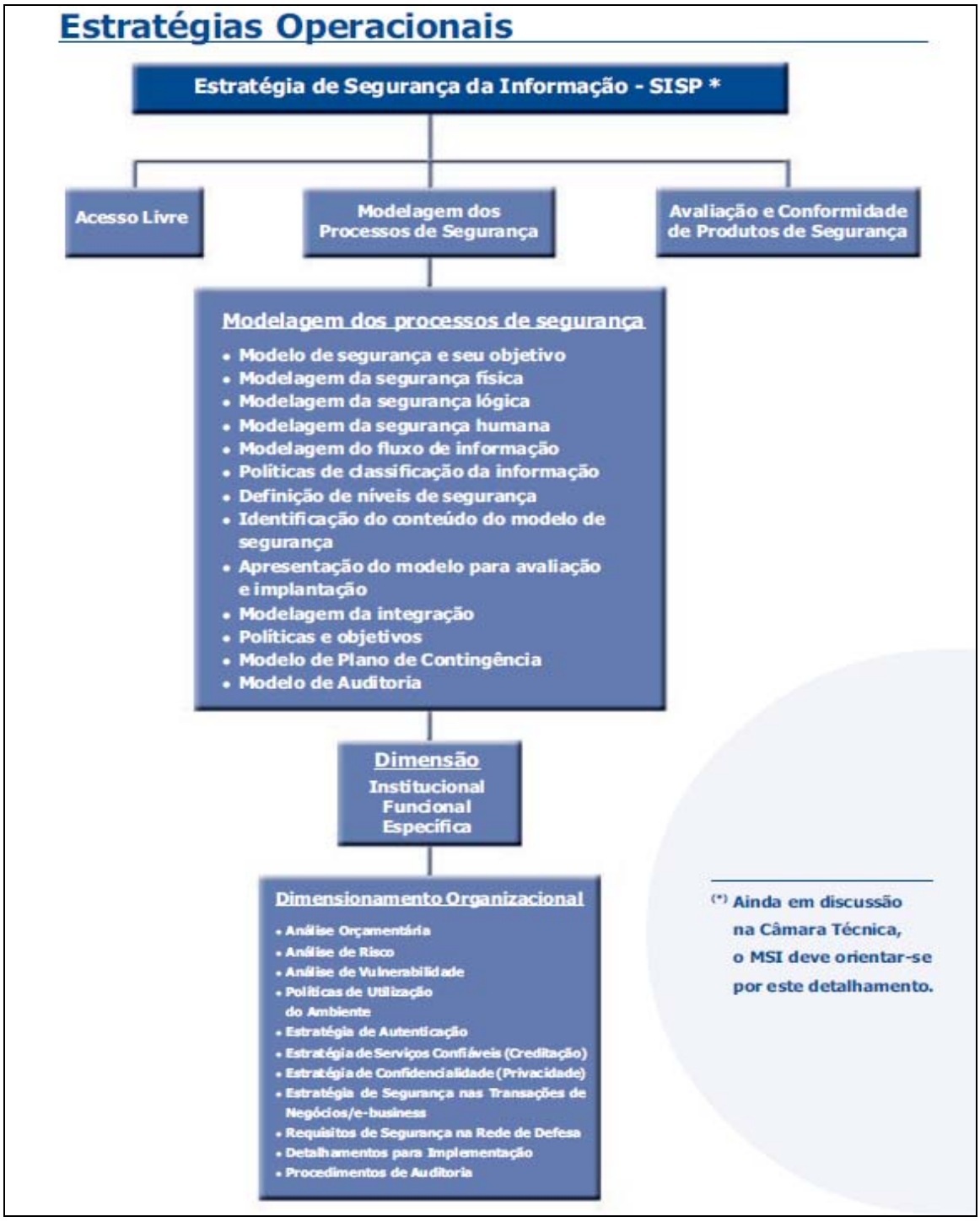

Figura 11 – Modelo da segurança de informação para administração pública

FONTE: LIMA, et al (2000)

3.2.1 Fases do modelo da segurança de informação

Segundo Miranda et al (2003) o modelo da segurança de informação (MSI) deve incluir as seguintes etapas: de avaliação, projecto, implementação, gestão, suporte, formação e conscientização em segurança da informação nos seus processos e produtos. Conforme ilustra a figura abaixo:

Figura 12 – Fases do MSI para administração pública

FONTE: LIMA, et al (2000)

- **Avaliação** – é a fase de análise das necessidades, procedimentos utilizados e a identificação dos processos críticos e análise de riscos e ameaças.

- **Projecto** – esta fase é responsável pela definição dos conceitos, da equipa responsável pela implementação e manutenção da segurança. Consiste ainda na elaboração de normas, procedimentos, plano de contingência, termo de compromisso e a divulgação do projecto para técnicos e utilizadores do sistema.

- **Implementação** – consiste na aplicação formal das regras e normas definidas na fase de projecto e a elaboração e implementação das modelagens a nível de segurança física, segurança humana, a segurança lógica e fluxo de informação.

- **Gestão** – é fase da descrição e levantamentos da situação actual do sistema. Implementação dos controlos de segurança, da revisão da política de segurança face as mudanças nos níveis de risco, avaliação e acção correctiva.

- **Suporte –** consiste na manutenção e monitorização de eficácia dos controlos de segurança.

Para os mesmos autores as fases do MSI devem ser avaliados e examinado periodicamente, levando em conta as normas e procedimentos que estão envolvidos, de acordo com as exigências tecnológicas imposta pela estruturação do *e-business* e do *e-commerce*, bem como qualquer aspecto que estejam em evolução.

3.3 Segurança em sistema de informação governamental em Cabo Verde

Segundo o Núcleo Operacional para Sociedade de Informação (NOSI), o sistema de informação governamental, foi criado juntamente com a Comissão Interministerial para a Inovação e Sociedade de Informação (CIISI) através da Resolução nº 15/2003 do Conselho de Ministros. O NOSI pertence ao Estado, e é o principal fornecedor de serviços do sistema de informação para o governo de Cabo Verde, e têm por missão propor e executar as medidas e política nas áreas da inovação, da sociedade de informação e da governação electrónica em Cabo Verde.

3.3.1 Sistemas de informação no Governo de Cabo Verde

As informações relativas aos Sistemas de Informação em Cabo Verde, foram fornecidas por um responsável da NOSI, no papel de Director geral da Tecnologia de Informação Eng. Senhor Lumumba.

Existem vários sistemas de informação desenvolvidos pelo NOSI no Governo de Cabo Verde de entre elas destacam os seguintes:

- **Sistema Integrado de Gestão Orçamental e Financeira (SIGOF)** – sistema desenvolvido pelo NOSI, para à gestão financeira do Estado de Cabo Verde, cujo objectivo é fazer o controlo orçamental, a gestão das despesas, das receitas e das contas públicas. Hoje este sistema permite a preparação, a execução e controlo dos orçamentos geral do Estado, possui um sistema único de cobrança (SUC) e uma interface que permite fazer o acompanhamento ao cidadão. Este sistema é uma ferramenta *Web-Oriented*, que possibilita a participação de forma descentralizada de todas as instituições públicas do Estado, nas diferentes fases de gestão orçamental e financeira.

- **Sistema Nacional de Identificação e Autenticação Civil (SNIAC)** – sistema que permite modernizar todos os sistemas de registos civis e centrais do país. Incorpora interface e bases de dados para disponibilizar e gerir cartão nacional de identificação. Este sistema permite os hospitais fazer pedidos de registos de nascimento on-line, permite as Câmaras Municipais intervir na requisição de registos prediais, permite também as embaixadas e serviços diplomáticas fazer emissão de certidões on-line e muitos outros serviços.

- **Sistema de Informação Municipal (SIM)** – também desenvolvido e implementado pelo NOSI, é o sistema que engloba a instalação de infra-estruturas informáticas, de centros de dados, redes locais, e sistemas de informação de todas áreas de gestão municipal, tais como taxas de impostos, licenciamentos, gestão de terrenos, gestão financeira, gestão de recursos humanos, etc. Permite a integração de municípios na rede do Estado mantendo-os ligados a Internet.

- **Sistema Eleitoral** – é o sistema que permite todos os cidadãos nacionais residentes no país a recensear-se. Possui interface de recolhas de assinaturas digitais, impressões e fotografias para os recenseamentos de cidadãos. Permite cadastral, registar e alterar os dados dos eleitores.

Existem muitos outros sistemas de informação no governo de Cabo Verde desenvolvidos pelo NOSI, cujo objectivo é melhorar a qualidade de serviços da administração pública com os clientes finais. Todos os sistemas acima mencionados foram desenvolvidos internamente, mas actualmente, o NOSI, sendo o único desenvolvedor dos sistemas de informação para o governo está a fazer subcontratação de empresas externas para desenvolver muitas outras aplicações para o Estado.

No que diz respeito a política da segurança o NOSI tem um protocolo assinado com a empresa *Microsoft*, no sentido de utilizar exclusivamente os *softwares* proprietários, para garantir a sua segurança.

Políticas da segurança para os clientes finais: são políticas da segurança definidas pelo NOSI no sentido de não possibilitar qualquer tentativa de acesso não autorizada por parte das pessoas não funcionários da instituição aos dados considerados sensíveis da instituição ou seja nenhuma pessoas ou empresas estranhas tem acesso aos dados da administração central da instituição.

O acesso aos servidores é restrito aos técnicos informáticos do NOSI, sendo estas protegidas por mecanismos de autenticação. Essa restrição é tanto a nível lógico como físico, tendo em conta que os servidores se encontram nas Instalações da instituição.

Em relação ao sistema de gestão de risco o NOSI, utiliza **a tecnologia ASA**, para gerir os riscos e ameaças que afectam os sistemas de informação governamental em Cabo Verde. Segundo um responsável do NOSI, **a Série Cisco ASA**, é uma plataforma de segurança mais moderna e eficiente para as redes organizacionais, que oferece os serviços de segurança de pequenas, médias e grandes empresas. Esta tecnologia possibilita a padronização em uma única plataforma permitindo a redução e gestão do custo operacional da segurança, a redução do custo com a formação do pessoal do quadro da instituição, e também a redução do custo com os equipamentos de reposição.

Ainda a tecnologia ASA, oferece serviços para a gestão e monitorização de dispositivos único, também oferece serviços de prevenção contra os intrusos nas redes do governo

protegendo assim das ameaças, como *worms*, *vírus*, ataques às aplicações e sistemas operacionais da administração pública.

Também utilizam **a tecnologia *BLUE COAT***, que segundo o mesmo responsável, é o maior provedor de aplicativos *WAN*, e oferece uma arquitectura de *proxy*, que torna o processo das instituições muito mais rápidos, reduzindo os riscos de segurança. Esta tecnologia traz grande vantagens para a administração pública uma vez que, permite melhorar os exercícios de recuperação de *backup* e segurança dos servidores. Também reduz os custos de gestão e infra-estrutura de tecnologia da administração pública.

Utilizam também dispositivos como *firewall* cujo objectivo é controlar o tráfego na rede do Estado.

Capítulo 4: O caso do MTIE

1 Enquadramento

O presente estudo, tem como intuito avaliar a situação actual da Segurança em Sistema de Informação governamental, mais precisamente no MTIE. Neste capítulo analisam-se os resultados obtidos através da entrevista informal (conversa aberta), recolha e análise de dados.

Tem-se como objectivo avaliar a situação actual dos Sistemas de informação governamental no Ministério do Turismo, Indústria e Energia do Governo de Cabo Verde, no que tange à análise e gestão de risco em segurança de informação. Especificamente, procura-se:

- Conhecer a situação da segurança de informação no Ministério do Turismo, Indústria e Energia – MTIE.

- Propor melhorias da segurança em Sistemas de informação no MTIE caso necessário.

Para a materialização do referido estudo foi utilizado como suporte as seguintes técnicas:

- Entrevista informal (Conversa aberta).

- Recolha e análise de dados.

2 O Ministério do Turismo, Indústria e Energia de Cabo Verde

O Ministério do Turismo, Indústria e Energia (MTIE) é um órgão governamental cujo objectivo é executar e avaliar as políticas públicas para as actividades económicas de produção de bens e serviços, no que diz respeitos às actividades industriais, à energia, ao comércio, ao turismo e às actividades de serviços às empresas. [5]

O MTIE foi criado recentemente pelo Governo de Cabo Verde após a última remodelação do Governo efectuado no ano 2010. Localiza-se ao Sul da ilha de Santiago mais concretamente na cidade da Praia, conhecido como cidade político-administrativa do país, zona de Achada Santo António, Rua Cidade do Funchal nº2.

Encontra-se a funcionar num prédio de quatros (4) andares, em regime de arrendamento, sendo no quarto piso, funcionam os serviços do gabinete da Ministra, assessor da Ministra e os dirigentes dos serviços autónomos e dos organismos da administração. No terceiro piso funcionam os serviços da direcção geral de planeamento, orçamento e gestão (DGPOG).

No segundo piso, funcionam os serviços da direcção geral de energia (DGE), no primeiro piso, funcionam os serviços da regulação de actividades económicas e no rés-do-chão funcionam os serviços da direcção geral de indústria e comércio (DGIC).

O Ministério vem prestando serviços na elaboração, coordenação e na execução de políticas públicas com impacto directo na competitividade da economia do nosso país, sobretudo no investimento público, na produtividade e melhoria do ambiente do negócio.

[5] www.mecc.gov.cv

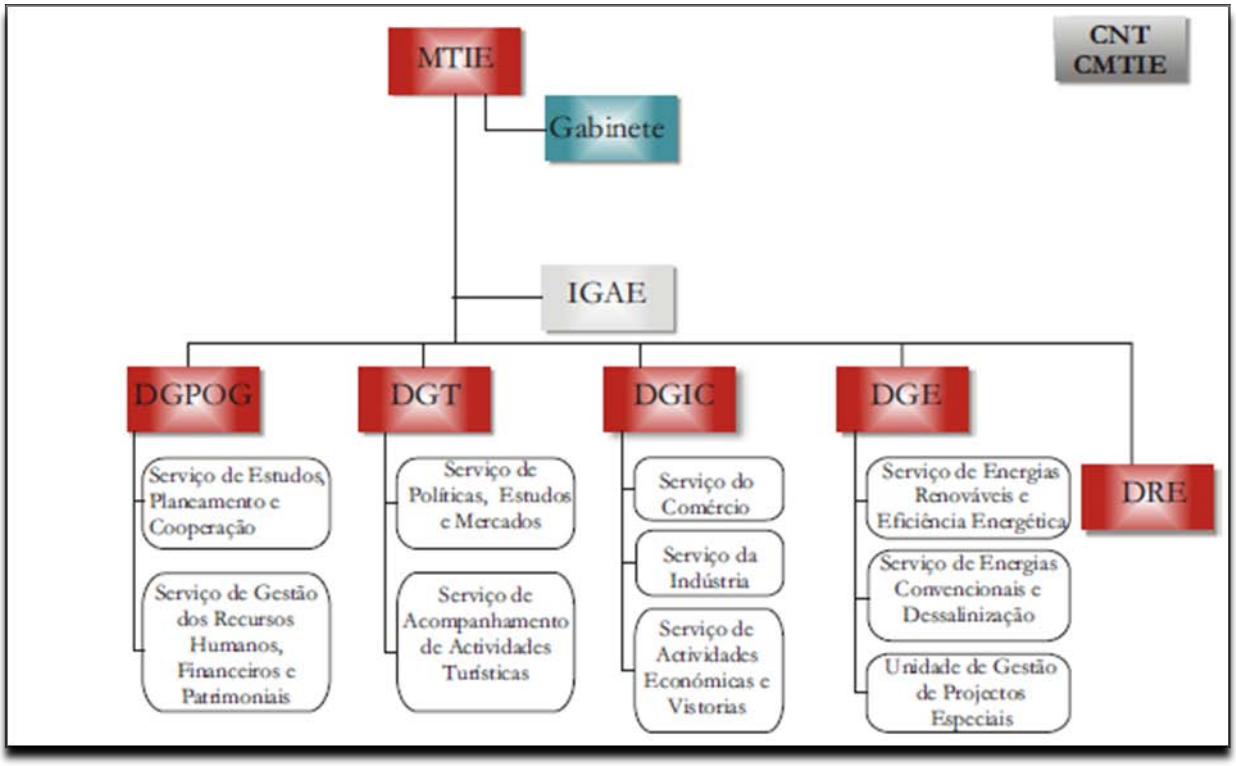

Figura 13 – Organigrama do MTIE

FONTE: Disponível em: www.mecc.gov.cv

2.1 Estrutura organizativa – os órgãos da administração e gestão

O MTIE, é constituído pelos respectivos órgãos:

O Conselho Nacional do Turismo – é o órgão consultivo para as grandes opções da política do turismo e sua relação com a política de desenvolvimento do país.

O Conselho do Ministério – é o órgão consultivo integrado pelo Ministros, pelos dirigentes dos serviços centrais do MTIE, pelos assessores do Ministro e pelos dirigentes dos serviços autónomos e dos organismos da administração indirecta sob superintendência do Ministro.

O Gabinete do membro do Governo – é o órgão que funciona junto do MTIE, cujo objectivo é assistir directa e pessoalmente, no desempenho das suas funções.

A Direcção Geral de Planeamento, Orçamento e Gestão (DGPOG) – é um serviço interdisciplinar e de apoio técnico, a quem compete a formulação e seguimento das políticas públicas de apoio técnico e administrativo na gestão orçamental, de recursos humanos, financeiros e patrimoniais do Ministério. Encontra-se integrada pelos seguintes serviços:

- **Serviço de estudos, planeamento e cooperação** – este serviço tem por missão prestar apoio técnico ao membro do governo na definição da política económica e no desenvolvimento de estudos e da recolha e tratamento de informação.

- **Serviço de gestão dos recursos humanos, financeiros e patrimoniais –** é o serviço de apoio e coordenação das politicas de desenvolvimento de recursos humanos e gestão administrativa e dos recursos financeiros, matérias e patrimoniais do MTIE, bem como da concepção e apoio técnico-normativo à formulação destas politicas e à sua monitorização e avaliação, num quadro de modernização administrativa, em prol da melhoria da qualidade do serviço público.

A Direcção geral da energia (DGE) – é o serviço responsável pela definição, concepção, execução e avaliação da política energética e de dessalinização, bem como pela apresentação de propostas visando o crescimento, a melhoria e o aumento da produtividade e competitividade do sector. Integra os seguintes serviços:

- **Serviço das energias convencionais e dessalinização** – responsável pelo funcionamento do sistema de energia e dessalinização, da segurança do abastecimento em condições de igualdade de tratamento, qualidade, competitividade e desenvolvimento durável amigo do ambiente.

- **Serviço das energias renováveis e eficiência energética –** é o serviço responsável pela promoção e colaboração de normas, regulamentos e especificações técnicas relativos a instalações de conversão de energias renováveis e de incremento da eficiência no uso da energia.

- **Unidade de gestão de projectos especiais –** assegura a gestão e execução de todas as actividades necessárias à concretização dos projectos sob sua responsabilidade, colaborando na execução de outras actividades inerentes ao seu âmbito de actuação.

Direcção geral da indústria e comércio (DGIC) – é o serviço responsável pela apresentação de propostas relativas à concepção, execução e avaliação das políticas sectoriais para a indústria e para o comércio, bem como pela coordenação em matérias relacionadas com a integração económica regional e cooperação internacional de índole bilateral ou multilateral. Ela integra os seguintes serviços:

- **Serviço da Indústria** – compete-lhe propor os planos e programas do sector da indústria e contribuir para a promoção da modernização e do desenvolvimento sustentado da competitividade das actividades industriais, numa perspectiva de incremento do valor acrescentado.

- **Serviço do comércio** – compete-lhe organizar, em colaboração com outros serviços e organismos competentes, estatísticas referentes ao sector comercial e divulgar informações de interesse para o desenvolvimento do mesmo. Na vertente externa assegura, em colaboração com outros organismos do Estado, a execução dos acordos estabelecidos e ratificados por Cabo Verde no âmbito do comércio.

- **Serviço de actividades económicas e vistorias** – garante o atendimento ao público em todas as áreas de competência do MTIE, funcionando num modelo de *Front Office.*

Direcção geral do turismo (DGT) – é o serviço responsável pela concepção, avaliação e execução da política do turismo, em estreita articulação com os serviços e organismos do sector. Ela integra os serviços de:

- **Serviços de politicas, estudos e mercados** – serviços que apoia o Governo na concepção e definição do modelo de politica para o sector do turismo.

- **Serviço de acompanhamento de actividades turísticas** – faz o acompanhamento e execução das acções voltadas para o desenvolvimento e o crescimento da actividade turística, através de pesquisas realizadas, em cooperação com outros serviços e organismos competentes.

Inspecção-geral das actividades económicas (IGAE) – é órgão e autoridade de polícia criminal em matéria de infracções antieconómicas e contra a saúde pública, que funciona sob a superintendência do Ministro do Turismo, Indústria e Energia, dotado de autonomia funcional, administrativa e financeira, bem assim dos necessários poderes de autoridade nos termos do respectivo Estatuto e demais legislação aplicável, ao qual compete velar pelo cumprimento das disposições legais que disciplinam as actividade económicas.

Direcção regional de economia (DRE) – é serviços do MTIE, cuja finalidade é a representação e actuação do MTIE a nível regional. As DRE representam o MTIE junto dos órgãos do poder local e articulam-se com os órgãos desconcentrados do poder central de incidência regional. Ainda tem como objectivo assegurar funções desconcentradas de execução das políticas do MTIE, em matéria de licenciamento, fiscalização e controlo metrológico, englobando as do sector do comércio e dos serviços, do turismo e da energia. Encontra-se dividida por:

- **Direcção regional norte (DREN)** – esta direcção tem sede em São Vicente e representa o MTIE nas Ilhas de São Vicente, São Nicolau e Santo Antão. Ela alberga as antenas do Cabo Verde Investimentos, da Agencia para o Desenvolvimento Empresarial e Inovação e os serviços da Inspecção-geral das Actividades Económicas.

- **Direcção regional centro (DREC)** – tem sede na ilha do Sal e representa o MTIE nas Ilhas de Sal e da Boa Vista. Ela engloba as antenas do Cabo Verde Investimentos, da Agência para o Desenvolvimentos Empresarial e Inovação e os serviços da Inspecção-geral das Actividades Económicas.

2.2 A infra-estrutura tecnológica do MTIE

Infra-estrutura tecnológica	Quantidade
Computadores	88
Servidor	1
Impressoras	5
Scanners	5
Máquinas fotocopiadoras	5
Videoprojectores	2
Retroprojectores	2

Quadro 1 – Infra-estrutura tecnológica do MTIE

O quadro acima representa a infra-estrutura tecnológica do MTIE. De acordo com os dados analisados o MTIE encontra-se bem apetrechado a todos os níveis, principalmente no que tange aos computadores. A ligação em rede permite a interligação entre os diferentes departamentos de modo a garantir o acesso rápido as informações fazendo com que o funcionamento da instituição seja o adequado.

Em relação à Internet o MTIE, possui uma largura de banda de cerca de 2MB/s garantindo a todos os colaboradores o acesso a aldeia global. Serviços W*ireless* não estão disponíveis neste Ministério.

2.3 Sistema de informação do MTIE

De acordo com os dados recolhidos, o MTIE possui actualmente os seguintes sistemas de informação:

Sistema de informação do MTIE
Tabela dinâmica
Título de comércio externo em linha (TC on-line)
Telefonia IP
Correio electrónico
Relógio de ponto

Quadro 2 – Sistema de informação do MTIE

De acordo com os dados analisados no quadro acima pode-se ver que o MTIE, dispõe de poucos sistemas de informação. Os sistemas de informação como tabela dinâmica e título de comércio externo em linha (TC – on-line) são fundamentais para a realização do trabalho na área do comércio e indústria. O relógio de ponto também é um sistema muito importante para o controlo de presença e segurança dos colaboradores do MTIE. Em relação a Telefonia IP e correio electrónico são sistema utilizados para a comunicação tanto interno como externo a instituição.

2.3.1 Tabela dinâmica

A tabela dinâmica é um aplicativo informático utilizado pelo MTIE para analisar a situação de todas as empresas do comércio e indústria licenciado na Câmara de Comércio de Sotavento em Cabo Verde.

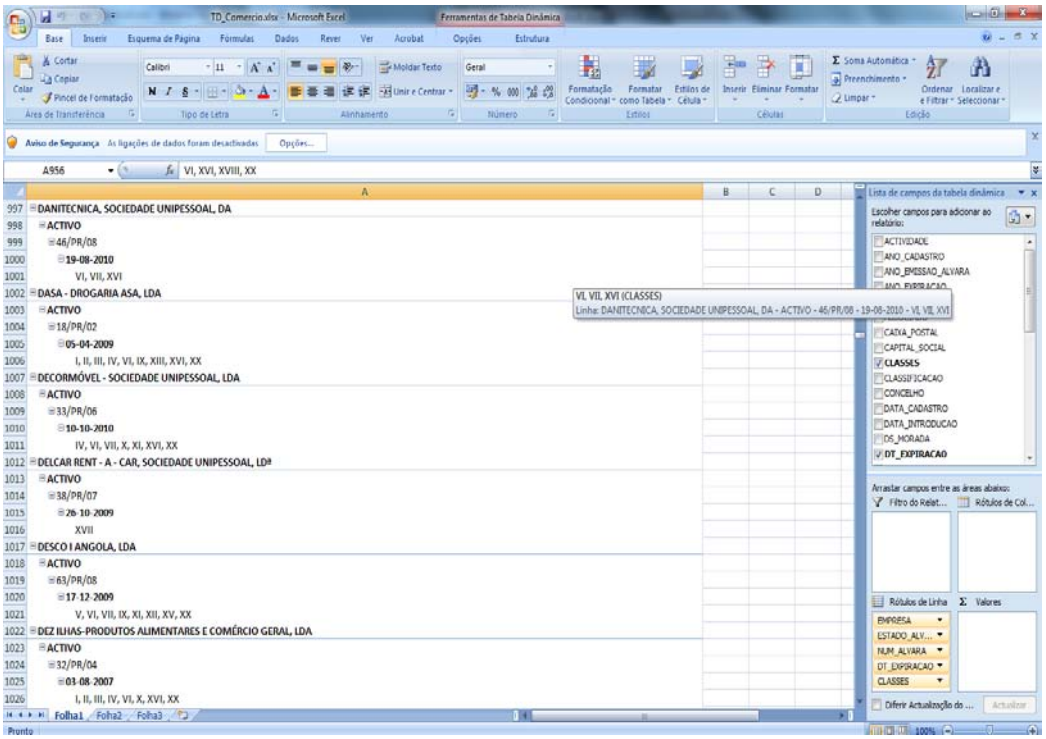

Figura 14 – Tabela Dinâmica

FONTE: MTIE (2010)

Nessa tabela, os dados são lançados por colaboradores da Câmara do Comércio de Sotavento no *site porton di nós ilhas*. Os colaboradores do MTIE utilizam este sistema para visualizar os dados lançados e avaliar a situação de todos os operadores licenciados. Este sistema permite saber o nome da empresa, em que ilha e concelho ficam a empresa, que tipo de empresa está cadastrado, que actividade executa, o seu estado de Alvará, o seu capital social, licença, contacto, número de identificação, números dos seus trabalhadores, quantidade ou volume de negócios e entre outras informações considerados pertinentes para o seu funcionamento.

Da análise aos dados da empresa no caso de anomalias a empresa será contactada pela direcção geral de indústria e comércio (DGIC), para a regulação do mesmo, caso contrário deixarão de fazer parte dos operadores licenciado na Câmara de Comercio de Sotavento.

2.3.2 Título de Comércio Externo (TCE- on-line)

É um aplicativo informático desenvolvido e utilizado pelo MTIE para satisfazer os pedidos de título de comércio externo em linha (TCE- on-line). Este pedido pode ser feito por nome de requerente, NIF ou ainda, pelo número do TCE on-line, como se pode ver na figura abaixo.

Figura 15 – TCE- on-line

FONTE: MTIE (2010)

Este sistema permite localizar um pedido TCE de forma mais rápida, sem percorrer a lista de pedidos disponibilizados manualmente. Para se ter acesso ao serviço de TCE, o utente deve estar cadastrado no portal. Para tal deve entrar no *site porton di nos ilha* através do endereço www.portondinosilha.cv e de seguida fazer a sua autenticação no portal introduzindo o *username* e *password.* Depois de se autenticar no sistema (*username* e *password*), o utilizador

deve fazer um clíque sobre o separador **D.G.COMERCIO**, e de seguida escolhe a operação desejada, de acordo com os módulos apresentados.

O TCE – on-line permite realizar um conjunto das actividades tais como: pedidos de TCE, pesquisa de um pedido TCE, ver informação do ciclo de vida do TCE, lista de artigos pautais, ver anexos TCE, bem como imprimir os TCE.

Em relação aos serviços do turismo e energia constata-se que a instituição trabalha a base do plano estratégico de desenvolvimento do turismo para o ano 2010/2013. Portanto todos os projectos já se encontram criados no concelho de Ministros, e o MTIE apenas executa os projectos de acordo com as suas prioridades. Nestas áreas, a instituição apresenta um grande défice em termos de utilização de algum sistema de informação para o apoio a realização dos serviços.

3 Políticas da segurança de informação no MTIE

3.1 Utilizadores, permissões e password

Todos os utilizadores do sistema para ter acesso as informações no MTIE, deve possuir um *login* e uma *password* criados pelo pessoal do sistemas de informação do NOSI. Quem deve fornecer os dados referentes aos direitos do utilizador é o responsável directo pela chefia, que deve preencher uma ficha e entregá-la ao departamento de recursos humanos e este entregar aos serviços central de NOSI que por sua vez faz o registo do utilizador. Se houver a necessidade de criação de um novo utilizador do sistema da instituição o responsável pelo novo utilizador deverá comunicar a sua necessidade ao NOSI, por meio de *email*, memorando ou telefone informando sobre as funções e necessidades em termos de *software* do novo funcionário.

O NOSI, ao fazer o registo do novo funcionário lhe informará sobre a sua nova *password*, e que este deve ser obrigatoriamente alterado após realizar a primeira entrado no sistema e ainda após isso, a cada final do mês, recomenda-se a mudança de *password* por questões de segurança.

3.2 Utilização de e-mail (correio electrónico)

Todos os funcionários devem utilizar as contas de correio electrónico institucional para comunicação tanto interno como externo mas, as mensagens escritas devem ter uma linguagem profissional de forma a não comprometer a imagem da instituição. O utilizador de sistema é o principal responsável por tudo o que é enviado pelo seu endereço, por isso é expressamente proibido enviar e abrir mensagens que prejudicam a imagem da instituição, mensagens com conteúdo perniciosos, difamatórias e que possam pôr em risco a integridade moral de qualquer parte envolvente na instituição.

3.3 Utilização de antivírus, novos sistemas, *softwares* e outros equipamentos informáticos

O NOSI, é o único responsável pelo serviço de actualização, manutenção e instalação de qualquer *software* no MTIE, não é permitido que os colaboradores façam actualização ou instalações de *software*, antivírus, ou outros nos seus computadores. Todos estes serviços são da responsabilidade do NOSI. Se houver a necessidade de instalação de qualquer *hardware ou software* o MTIE, tem a obrigatoriedade de comunicar a NOSI.

3.4 Utilização da linha telefónica

Todos os colaboradores têm permissão de utilizar a linha telefónica disponível nos serviços do MTIE. O responsável pelo controlo e permissões é o próprio MTIE que se encarrega de aplicar as restrições caso entender que o uso do mesmo coloca em risco a gestão ou a administração da instituição. Todo o final do mês é produzido o relatório de gasto da linha telefónica ao MTIE com intuito de avaliar o valor gasto pela instituição.

3.5 Acesso ao prédio

A segurança do acesso ao prédio é garantido através de um sistema de vigilância e segurança na porta central do Ministério que permite controlar a entrada e saída das pessoas no estabelecimento de serviço. O serviço é reforçado ainda com uma guarda responsável pela orientação e encaminhamento do pessoal ao serviço do MTIE. Também a segurança do prédio durante dia e noite é garantida por uma empresa de vigilância e segurança.

3.6 Acesso ao servidor

A sala do servidor fica situada no último piso e com uma única porta de acesso e encontra-se climatizado com uma temperatura de ar condicionado de acordo com as normas. O acesso a sala de servidor é autorizado apenas ao responsável dos serviços tecnológicos do MTIE e do NOSI. Uma vez dentro da sala, o acesso ao servidor só é permitido mediante autenticação (*username e password*). É expressamente proibido o acesso a sala de servidor por pessoas estranhas.

4 Planos de segurança

4.1 Cópia de segurança dos dados – *Backups*

Todos os serviços de *backup* é garantida pelo NOSI, e são feitas semanalmente. Após a realização do *backup* de informação o NOSI enviará cópias do mesmo para a administração do MTIE, e estes vão sendo armazenadas em local seguro longe do centro do processamento de dados de modo a evitar uma eventual perda de informação no caso de ocorrer um desastre. Todos os *backup* realizados por serviço de NOSI, é protegido com *password* de modo a evitar que os colaboradores tenham acesso não autorizado. Também todos os *backups* guardados fora da instituição devem ser mensalmente testado pelo pessoal do NOSI acompanhada do responsável de Tecnologias de informação do MTIE, no sentido de verificar se todas as informação guardadas estão operacionais.

4.2 Serviços de Seguros

No MTIE existe uma política de seguro em que todos os equipamentos informáticos encontram-se segurados contra as perdas e danos matérias. Num eventual dano dos recursos informáticos a empresa seguradora tem por obrigação cobrir todos os prejuízos causados.

4.3 Sistema de Prevenção de acidente

O sistema de prevenção de acidente é assegurado por uma empresa exterior contratado pelo MTIE. Em todas as salas do MTIE encontra-se equipadas com equipamentos de combate à incêndio. O serviço de manutenção é encarregado ao pessoal da empresa contratada que no

final de cada mês fazem a manutenção e vistoria dos equipamentos no sentido de atestar o seu estado de funcionamento.

5 Segurança dos recursos humanos

5.1 Controlo de presença e segurança do pessoal

No que concerne ao sistema de controlo de presença e segurança do pessoal, o MTIE, dispõe de um sistema denominado de Relógio de ponto que permite o controlo da entrada e saída de todos os colaboradores na respectiva instituição. Ver a figura abaixo.

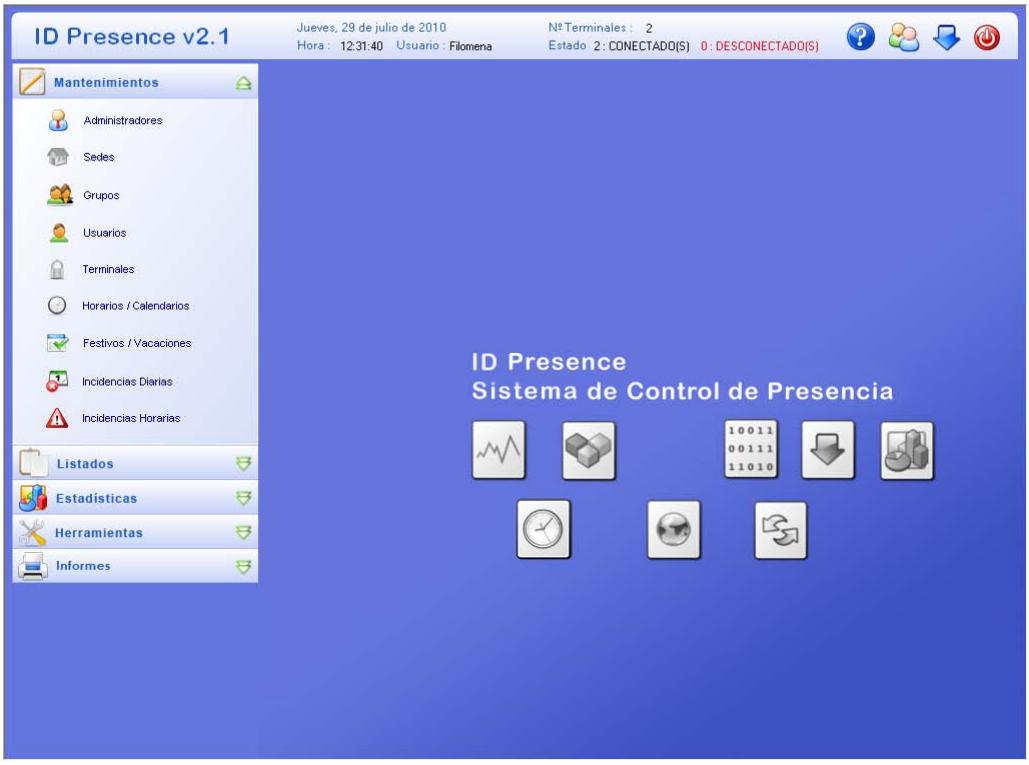

Figura 16 – Relógio de ponto

Através deste sistema o administrador do mesmo faz o registo de todos os colaboradores do MTIE, através do preenchimento de um formulário adequado por parte do funcionário ou do estagiário. De acordo com o tempo de serviços das duas categorias vai se proceder a autenticação do mesmo, sendo que quando terminar o tempo de contrato estabelecido por

estes profissionais o sistema desactiva automaticamente deixando em aberto a possibilidade da reactivação desta.

O sistema permite fazer registos das entradas e saídas através de impressão digital ou através de código de acesso. O registo de entrada e saída através de impressão digital processa da seguinte forma: o funcionário após ser registado no sistema, coloca o dedo no aparelho de registo localizado na porta pressionando-o até ouvir o sistema dizer acesso permitido ou não. Em relação ao código de acesso o funcionário digite o seu código de identificação e a sua *password* esperando pelo acesso permitido por sistema.

O sistema ainda dá a possibilidade de fazer registo para um conjunto de opções como: opção 1 Almoço; opção 2 Reunião; opção 3 Consulta Médica; opção 4 Assunto pessoal e opção 5 Deslocação em missão de serviços.

No final de cada mês o sistema permite gerar relatórios de faltas tanto a nível individual como em grupo de todos os colaboradores do MTIE.

5.2 Processo de recrutamento

Ainda em relação a segurança do pessoal, sabe-se que todo o processo de recrutamento é realizado de acordo com a lei vigente e mediante o anúncio do concurso público, e é realizado pelo departamento de recursos humanos.

5.3 Protecção da informação dos colaboradores

O MTIE, é o principal responsável pela protecção das informações dos seus colaboradores. Ele proíbe e sanciona qualquer colaborador da instituição que utilize as informações de terceiro (Cliente) para fins diferentes do interesse da instituição ou da própria pessoa e que ponham em risco a segurança deste. Não é permitido fazer a transferência da informação dos clientes para terceiros sem a autorização prévia do MTIE, ou seja isso só se faz caso o MTIE entender que é benéfico tanto para o cliente como para o serviço da instituição.

5.4 Promoção e mudança de função

Na presença de promoção de um colaborador para outras funções o departamento de recursos humanos devem informar com antecedência o serviço de NOSI, no sentido de mudança de acessos aos serviços para qual foi promovido. Também todas as informações existentes no anterior posto de trabalho do colaborador promovido devem ser eliminados no intuito de garantir a segurança das suas informações.

6 Proposta de melhoria

O MTIE, depara-se com alguma carência dos sistemas de informação na área do turismo e energia. Por isso deve apostar na introdução de um sistema de informação integrada que permite melhorar a comunicação e relacionamento com as empresas do turismo e energia tanto privada como pública.

Uma opção viável seria a implementação de uma interface interactivo que permite a instituição obter informação, conhecer e comunicar com todas as empresas do turismo e energia existente no país. Esta proposta pode não ser bem sucedido sabendo que a introdução do sistema de informação numa organização implicará aumento elevado do custo para a instituição, mas também, a introdução de um interface pode melhorar a qualidade e o relacionamento na prestação de serviços da instituição.

Em relação aos serviços do comércio e indústria, elas estão bem sistematizados pelo que não é necessário o aumento ou a melhoria do mesmo, mas denota-se algumas dificuldades por parte dos colaboradores em utilizar esse sistema, por isso propõe que todos os utilizadores desses sistemas passassem por um processo de formação específica de modo a saber utilizar o sistema.

O MTIE, mesmo tendo o NOSI, como responsável pela prestação de serviços de infra-estrutura tecnológico e sistema de informação, deve recorrer a uma outra opção, isto por causa da morosidade do NOSI na prestação do serviço. Esta opção deve passar pela aposta no recrutamento ou na formação de um técnico na área de informática ao qual permite resolver problemas pontuais que surgem durante os serviços.

Constata-se, através da recolha e análise de dados, que ao nível da segurança de informação no MTIE os colaboradores estão bem sensibilizados, mas conclui-se que não existe directrizes claras que penaliza os colaboradores a não cumprimento das políticas de segurança da informação definida pelo MTIE.

Por isso, a partir deste facto, propõe-se ao MTIE a definição de um documento formal que descreve as sanções levadas a cabo pelo não cumprimento das políticas da segurança de

informação definida pela instituição, nomeadamente suspensão e/ou rescisão do contrato de trabalho por parte dos colaboradores.

7 Recomendações

Com base nos dados recolhido e analisado conclui-se que o NOSI tem optado por uma política de utilização do *software* proprietário como estratégia da segurança de informação, cujo investimento requer custo elevado para a obtenção de licença da sua utilização.

Neste contexto, recomenda-se ao NOSI, a optar por uma política de utilização do *software* livre em detrimento do *software* proprietário por seguintes razões:

Segundo Silva et al (2005) os *softwares* livres são:

- Disponibilizados gratuitamente, ou comercializado com as premissas de liberdades e instalações, plena utilização, acesso ao fonte, possibilidade de modificação/aperfeiçoamento para necessidades específicas e a distribuição de forma original ou modificada com ou sem custo, por isso o governo ao utilizar esse tipo de *software* está a contribuir para a redução do custo do investimento em relação a utilização do *software* proprietário;

- Os *softwares* livres possibilitam a adopção de padrões abertos para o governo electrónico (e-Gov);

- A utilização de *software* livre faz com que o governo não depende de um único fornecedor;

- Os *softwares* livres permitem a eliminação de mudanças compulsórias que os modelos proprietários impõem periodicamente a seus utilizadores, em face da descontinuidade de suporte a versões ou soluções.

Segundo Osório et al (2005) a existência do *software* livre de qualidade e disponível no mercado será uma boa solução para qualquer organização, sobretudo para as instituições públicas onde os recursos financeiros disponibilizados são sempre escassos. A utilização desse *software* permitirá economizar recursos financeiros gastos para a obtenção e licenciamento de s*oftware* proprietário e os recursos economizados poderá ser utilizados para outros fins dentro da instituição.

Conclusão

Ao longo deste trabalho fica claro que o sucesso de uma organização depende dos sistemas de informação e da sua segurança. A introdução do sistemas de informação nas organizações mudaram a forma de recolher, processar e transmitir a informação, e estas por conseguinte, trouxeram grande evolução no campo da segurança de informação.

No que refere a segurança em sistema de informação constata-se que os elementos da segurança de informação como disponibilidade, confidencialidade, integridade, não repudiação, autenticidade e controlo de acesso são características indispensáveis para o aumento da segurança de qualquer organização.

Concluiu-se que o processo de análise de risco é muito importante para a questão da segurança de informação em qualquer organização, isto porque através deste processo a organização consegue verificar e analisar o nível de risco que a organização está a enfrentar e através deste fazer uma ponte entre o que se quer proteger e o que se tem para proteger, também este processo ajuda a organização a estabelecer um orçamento adequado para a questão da segurança de informação na organização.

Também conclui-se que é fundamental o papel da política de segurança numa instituição uma vez que, estes permitem todos os colaboradores conhecer quais as normas e regras a respeitar dentro da instituição.

Em relação a segurança em sistema de informação no governo conclui-se que é importante adoptar um modelo de segurança que consegue dar resposta eficaz e eficiente na política do governo.

De acordo com os dados recolhido e analisado chega-se a conclusão que no que concerne ao sistema de informação no MTIE, existem algumas necessidade da melhoria, mencionadas nas propostas de melhorias, como é caso das áreas de Turismo e Energia.

No entanto, existem alguns aspectos de mais-valia e que merecem destaque no MTIE mais concretamente na área do comércio e indústria, porque existem neste Ministério sistemas de informação que está a satisfazer os objectivos da instituição.

- Na área de comércio e indústria os colaboradores utilizam **Tabela dinâmica** que é um aplicativo que permite analisar a situação de todas as empresas do comércio e indústria licenciado na Câmara de Comércio de Sotavento em Cabo Verde.

- Também utilizam **TC- On-line**, aplicativo que permite satisfazer os pedidos de título de comércio externo em linha (TCE- on-line).

Tendo em conta a grandeza do MTIE, e o seu campo de actuação a aposta na segurança em sistemas de informação é fundamental para o aumento da competitividade da Instituição. Dentro deste contexto conclui-se que é extremamente importante que todos os colaboradores deste sistema tenham os seguintes conhecimento ao nível da segurança exigida pela instituição:

- Todos os colaboradores devem preencher os requisitos mínimo exigidos (*Username e password*) para ter acesso a informação no MTIE;

- Todos os colaboradores devem conhecer e respeitar as políticas de utilização de *email*, *password*, antivírus e software/programas estabelecidas pela instituição;

- Todos os colaboradores devem ter o conhecimento que o sistema de *backup* é da inteira responsabilidade do NOSI;

- Todos os colaboradores têm direito a protecção das suas informações dentro da instituição.

Em título de conclusão queria deixar uma mensagem de motivação às autoridades políticas que sustentam o nosso governo no sentido de continuarem a apostar firmemente no processo da introdução do sistema de informação no governo que possam torná-la mais seguro e mais competitivo, com sistemas mais actualizados e que estendem-na a toda franja do governo.

Aos profissionais desta área uma palavra de encorajamento no sentido de abraçarem com todo o amor a área da segurança informática e que façam um bom uso do conhecimento para o bem do país.

Bibliografia

BOGHI, Cláudia & SHITSUKA, Ricardo. (2002). *Sistemas de Informação: Um enfoque dinâmico.* São Paulo: Editora Érica.

CARNEIRO, Alberto. (2002). *Introdução à Segurança dos Sistemas de Informação.* Lisboa: Editora da informática.

Constituição da República de Cabo Verde. (2007). Praia. Editora: Assembleia Nacional.

ED. Titel. (2003). *Teoria e problemas de rede de computadores*. Porto Alegre. Editora: artmed S.A.

FERREIRA, Jorge. (1995). *Manual técnico de segurança dos sistemas e tecnologias de informação.* Editora: Instituto de informática.

FOROUZAN, Behrouz A. (2006). *Comunicação de dados e redes de computadores*. Porto Alegre: Bookman. 3. Edição.

ILTEC. (1993). *Dicionários de termos informáticos*. Lisboa: Edição Cosmos.

ISAÍAS, Pedro. (2001). *Análise de Sistemas de Informação*. Lisboa – Palácio Ceia – Rua da Escola Politécnica.

LAMAS, Estela P.R et al. (2001). *Contributos para uma metodologia Científica mais Cuidada*, Lisboa. Editora: Instituto Piaget.

LOPES, C. Filomeno et al. (2005). *Desenvolvimento de sistema de Informação.* Lisboa: Editora de Informática.

MAGALHÃES, Hugo & GRILO, Alberto. (2006). *A segurança informática e o negócio electrónico*. Porto. Editora: SPI- Sociedade Portuguesa de Inovação, S.A.

MAMEDE, S. Henrique. (2006). *Segurança informática nas organizações*. Lisboa: Avenida Praia da Vitoria, Porto: Rua Damião de Góis, Coimbra: Avenida Emídio Navarro. Editora de informática, Lda.

MONTEIRO, Edmundo et al. (2000), *Engenheira de Redes Informática*, Lisboa. Editora Informática Lda.

MORAES, F. Alexandre & CIRONE, C. António. (2003). *Redes de computadores: da Ethernet à Internet.* São Paulo. Editora: Érica.

RASCÃO, José. (2001). *Sistemas de Informação para Organizações – a informação chave para tomada de decisão.* Lisboa: Edições Sílabo, Lda.

RODRIGUES, Luís Silva. (2002). *Arquitectura dos Sistemas de Informação*. Lisboa: Editora de Informática.

SAWAYA, R. Márcia. (1999). *Dicionário de informática & Internet*. São Paulo. Editora: Nobel.

SILVA, R. Elcelina. (2005). *Perfil de Utilizador em Redes Locais*. Praia.

SILVA, R. Elcelina. (2006). *Redes Universitários Segurança e Auditoria*. Praia.

TORRES, B. Catarina et al. (2003). *Segurança dos sistemas de informação: Gestão estratégica da segurança empresarial.* Lisboa: Portugal.

VARAJÃO, Q. E. João. (2000). *Planeamento de Sistema de Informação*. Lisboa: Editora de informática.

ZÚQUETE André. (2006). *Segurança em redes informáticas.* Lisboa: Avenida Praia da Vitoria, Porto: Rua Damião de Góis, Coimbra: Avenida Emídio Navarro. Editora de informática, Lda.

Paginas Web

AURELIO, Marco. (2005). *A continuidade de negócio e o plano de recuperação*. Disponível <http://www.malima.com.br/article_read.asp?id=170> [Consultado em 18-05-2010].

BASTOS, R. Eri. (2005). *Politica de segurança.* Disponível <http://www.linuxman.pro.br/node/7> [Consultado em 20-05-2010].

BAZZOTTI, Cristiane & GARCIA, Elias. (s/d). *A importância do sistema de informação gerêncial para tomada de decisões*. Disponível: <http://www.unioeste.br/campi/cascavel/ccsa/VISeminario/Artigos%20apresentados%20em%20Comunica%C3%A7%C3%B5es/ART%203%20%20A%20import%C3%A2ncia%20do%20sistema%20de%20informa%C3%A7%C3%A3o%20gerencial%20para%20tomada%20de%20decis%C3%B5es.pdf> [Consultado em 27-04-2010].

BEUREN, Maria Ilse & MARTINS, Waltrick Luciano. (2001*). Sistema de Informações Executivas: Suas Características e Reflexões sobre sua Aplicação no Processo de Gestão.* Disponível: <http://www.eac.fea.usp.br/cadernos/completos/cad26/Revista_26_part_1.pdf> [Consultado em13-04-2010].

CHAVES, C. O. Eduardo & FALSARELLA, Mina Orandi. (2008). *Sistemas de Informação e Sistemas de Apoio à Decisão.* Disponível <http://www.chaves.com.br/TEXTSELF/COMPUT/sad.htm> [Consultado em13-04-2010].

CIMA, Fernando. (s/d). *Segurança na Microsoft. Comentários e análises sobre a segurança da informação*. Disponível <http://blogs.technet.com/fcima/archive/2006/10/05/Como-Definir-sua-Pol_2600_iacute_3B00_tica-de-Senhas.aspx> [Consultado em 18-05-2010].

CLESIO, Flavio. (2008). *Segurança de informação – Básico.* Disponível: <http://info.abril.com.br/forum/viewtopic.php?f=122&t=371> [Consultado em 03-05-2010].

COSTA, E. Carlos. (2007). *Sistema de informação – sistemas de gestão empresarial.* Disponível: <http://www.administradores.com.br/informe-se/producao-academica/sistemas-de-informacao-sistemas-de-gestao-empresarial/358/> [Consultado em 08-04-2010].

FAURI, T. Roberto. (2009). *Adote uma politica de segurança em seu computador – parte 1*. Disponível <http://www.dinx.com.br/2009/10/adote-uma-politica-de-seguranca-em-seu-computador-parte-1/> [Consultado em 18-05-2010].

FAVERO, Luz Hamilton et al. (2006). *Sistema de informação contábil e a sua importância para o controle dos bens permanentes do sector público.* Disponível <http://www.dcc.uem.br/enfoque/new/enfoque/data/1180136954.pdf> [Consultado em 16-06-2010].

FILHO, S. M. António. (2004). *Segurança da Informação: Sobre a Necessidade de Protecção de Sistemas de Informações.* Disponível: <http://www.espacoacademico.com.br/042/42amsf.htm> [Consultado em 03-05-2010].

FREITAS, H. et al. (2001). *Sistemas de informações: Um estudo comparativo das características tradicionais às actuais.* Disponível: <http://www.gestaosocial.org.br/conteudo/quemsomos/ensino/area-restrita/turma-3/se-3-estrategias-e-instrumentos-de-desenvolvimento-e-requalificacao-territorial/avaliacao-e-sistemas-de-suporte-a-decisao/textos-prof-jair-sampaio-soares-jr/textos-para-leitura/Sistemas%20de%20informacoes%20-%20um%20estudo%20comparativo%20das%20caracteristicas%20tradicionais%20as%20atuais..pdf> [Consultado em 13-04-2010].

Glossário de Segurança da Informação e Internet. Disponível <http://www.smartsec.com.br/glossario_seguranca.html> [Consultado em 31-05-2010].

GOUVEIA, B. M. Luís. (s/d). *Sistema de Informação.* Disponível: <http://www2.ufp.pt/~lmbg/textos/si_texto.pdf> [Consultado em 08-04-2010].

LAUREANO, P. A. Marcos. (2005). Gestão de segurança da informação. Disponível: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf> [consultado em 03-05-2010].

LAURO, José & FREITAS, M. V. Marcus. (s/d). *Politicas de segurança da informação.* Disponível <http://www.viniciusmaia.com.br/wp-content/uploads/2009/07/Artigo-PoliticaSeguranca.pdf> [Consultados em 14-05-2010].

LIMA, Oliveira de N. José et al. (2000). *Fundamentos do Modelo de Segurança da Informação.* Disponível<http://www.redegoverno.gov.br/eventos/arquivos/Mod_Seg_Inf.pdf> [Consultado em 16-06-2010].

LUZ, C. J. Carlos. (2009). *Sistema de informação.* Disponível <http://moodle.cv.unipiaget.org/course/view.php?id=44 > [Consultado em 22-04-2010].

MACÊDO, C. Rodrigo & TRINTA, M. A. Fernando. (1998). *Um estudo sobre Criptografia e Assinatura Digital.* Disponível <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm> [Consultado em 31-05-2010].

MEDEIROS, R. D. Carlos. (2001). *Implantação de medidas e ferramentas de segurança da informação*. Disponível <http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf> [Consultado em 05-04-2010].

MIRANDA, Amaral Rafael et al. (2003). *Segurança da Informação no Governo Federal: O caso do Cartão Nacional de Saúde do SUS.* Disponível <http://www.lyfreitas.com/artigos_mba/cns2.pdf> [Consultado em 22 -06-2010].

MONTEIRO, Oliveira. C. L. Iná. (2009). *Proposta de um Guia para Elaboração de Políticas de Segurança da Informação e Comunicações em Órgãos da Administração Pública Federal.* Disponível < http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/ina_lucia.pdf> [Consultado em 13-04-2010].

NAÇÕES Unidas. (1995). *Government Information System, A guide to effective use of information technology in the public sector of developing countries.* New York: Disponível <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan000155.pdf> [Consultado em 22 -06-2010].

PEREIRA, Brito. F. Valdo. (2006). *Apoio à Administração, Business Intelligence.* Dísponivel:<http://bdigital.unipiaget.cv:8080/dspace/bitstream/123456789/89/1/Valdo%20Pereira.pdf> [Consultado em 12-05-2010].

PINHEIRO, S. M. José. (2007). *Conceitos de Redundância e Contingência*. Disponível <http://www.malima.com.br/article_read.asp?id=377> [Consultado em 18-05-2010].

PROMON, Business & Tecnology Review. (2005). *Segurança da informação: um diferencial determinante na competitividade das comparações.* Disponível: <http://www.promon.com.br/portugues/noticias/download/Seguranca_4Web.pdf> [consultado em 03-05-2010].

SILVA F. José. (s/d). *Sistema de Informações Gerências e a Contabilidade de Custos.* Disponível: <http://www.sappiens.com/pdf/comunidades/contabilidad/SIG_CONT_sappiens.pdf> [Consultado em 19-04-2010].

SILVA, F. Candido. (s/d). *Segurança em sistemas de informação.* Disponível <http://ensino.univates.br/~chaet/Materiais/apres-candido-completa.pdf> [Consultado em 29-04-2010].

SILVA, L. I. Luiz et al. (2005). *Guia Livre. Referência de Migração para Software Livre do Governo Federal / Organizado por Grupo de Trabalho Migração para Software Livre*. Brasília. Disponível < http://www.softwarelivre.gov.br/documentos-oficiais> [Consultado em 29-09-2010]

SILVA, V. Cristiano. (2005). *Proposta de um sistema de apoia à decisão para supermercado.* Disponível: <http://www.mba.unifei.edu.br/tccs/TCCMBA04Cristiano.pdf> [Consultado em 27-04-2010].

SOUZA, J. Rubens. (2001). *Implementação de servidor web seguro com windows server 2003 para a empresa caixa económica federal*. Disponível <http://www.rjs.eti.br/arq/TCC_RubensSouza.pdf> [Consultado em 25-05-2010].

SPANCESKI, R. Francini. (2004). *Política de segurança da informação – Desenvolvimento de um modelo voltado para instituições de ensino.* Disponível <http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf> [Consultado em 14-05-2010].

OSÒRIO, G. L. Tito et al. (2005). *Utilização de Software Livre em órgãos Públicos.* Disponível http://www.aedb.br/seget/artigos05/360_Artigo_SL_Completo.pdf [Consultado em 30-09-2010]

VARICAN. (1999). Governos. Disponível <http://www.varican.xpg.com.br/varican/Bpolitico/governo.htm> [Consulta 03-06-2010].