PRINCÍPIOS EM SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

Jonas K. Kahumba

Mestrado em tecnologia da informação

UNIDA

Assunción, Paraguay

E-mail: eng.kahumba@gmail.com

RESUMO: O presente artigo tem como principal objectivo verificar em que medida as pequenas e médias empresas realizam gestão da segurança da informação, evidenciar a necessidade de que novas práticas, uso das tecnologias de informação nas organizações como ferramentas de apoio e Baseia-se na reflexão acerca do cenário actual, da inserção das TI em diferentes sectores das organizações, também identificar os principais factores que influenciam as organizações na segurança de informação ,uso das melhores práticas de segurança nas informações nas organizações aplicandos as normais de politicas de segurança ABNT NBR ISO/IEC 27001:2006[1].

Palavras-chave: TI, Gestão de segurança, Segurança de Informação

RESUMEN: En este artículo se pretende comprobar en qué medida las empresas pequeñas y medianas empresas se dan cuenta de la gestión de seguridad de la información, poniendo de relieve la necesidad de nuevas prácticas, el uso de tecnología de la información en las organizaciones como herramientas de apoyo y se basa en la reflexión acerca de la situación actual de la integración en diferentes sectores de las organizaciones también identificar los principales factores que influyen en las organizaciones de seguridad de la información, el uso de las mejores prácticas de seguridad de la información en las organizaciones políticas de seguridad normales aplicandos ISO / IEC 27001: 2006.

Palabras clave: gestión de la seguridad de TI, Seguridad de la Información

[1] Jonas K. Kahumba ,Mestrado em tecnologia da informação
UNIDA, Assunción, Paraguay, E-mail: eng.kahumba@gmail.com (2016)

Introdução

O mundo actual é designado por **era de informação** ou **era de conhecimento** , isto porque toda a organização ,independentemente da sua categoria, tem como a informação como chave na manipulação da organização servindo como o elemento chave na produção das organizações . Hoje já é notável o uso das tecnologias de informação e comunicação em diferentes sectores das organizações como ferramentas de apoio aos funcionários e melhores praticas na prestação de serviço. A segurança de informação deve ser vista como uma componente principal da gestão de informação numa organização por ser elemento chave da estratégia do negocio das organizações [2].

Segurança da Informação Segurança da informação, conforme Beal (2005), é o processo de protecção da informação das ameaças a sua integridade, disponibilidade e confidencialidade. Sêmola (2003) define segurança da informação como "uma área do conhecimento dedicada à protecção de activos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade." A ISO/IEC 17799:2005, em sua seção introdutória define segurança da informação como "a protecção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Assim, podemos definir segurança da informação como a área do conhecimento que visa à protecção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos.

A Segurança da Informação nas Organizações

Actualmente, não se pode afirmar que nenhuma organização possui as medidas de protecção suficientes para se tornar segura. Cada vez mais se assiste a uma diversidade de ataques que exploram vulnerabilidades de software, aplicacional ou de sistema operativo. Os ataques mais frequentes são os de acesso remoto, as backdoors

---

[2] Jonas K. Kahumba ,Mestrado em tecnologia da informação,UNIDA ,Assunción, Paraguay E-mail: eng.kahumba@gmail.com ,2016)

aplicacionais, os erros de sistema de operativo, as bombas do correio electrónico, os vírus e o spam[3].

Modelos e Políticas de Segurança nas Organizações

A política de segurança, dentro de uma organização, vai designar a segurança de determinado sistema e esta pode ser formal ou informal. Quando falamos em modelos de segurança, estamos a referir-nos a uma política de segurança em particular, ou então a um conjunto de políticas. Nos modelos de segurança utilizam-se linguagens formais para a sua explicação[4]. As fontes para o desenvolvimento de uma política são variadas, pois intervêm os factores internos e os factores externos. Assim sendo, internamente deve ser analisada a missão e os objectivos da organização, as funções existentes, os riscos, as ameaças, os recursos financeiros e todos os outros factores que constituem a empresa. Externamente os riscos também devem ser analisados, bem como os custos e até mesmo as questões legais. Uma política de segurança não pode nunca caracterizar-se por ser estática, visto que, a sua adaptação às novas realidades que vão surgindo na empresa é fundamental, devendo ainda conseguir adaptar-se às mais diversas situações que sucedem. Ora, como já se referiu, os modelos de segurança que são integrados na organização formalizam as políticas implementadas, sendo descritas as regras a adoptar. Irão, por isso, ser apresentados modelos por vários autores, tendo em conta que os modelos podem ser qualificados por "confidencialidade, integridade, híbridos, composição e não interferência e baseados em critérios do senso comum". Os modelos mais populares são o Modelo de BellLaPadula, o modelo de Harrisson-Ruzzo-Ullman, o modelo Chinese-Wall, o modelo de Biba, o modelo de Goguen-Meseguer e o modelo de Sutherland. Para implementar a política devem ser seguidas várias etapas (Hartley e Locke, 2001), sendo a primeira a avaliação e entendimento das necessidades de segurança, depois se já existirem políticas estas devem ser revistas. A terceira etapa consiste em definir os requisitos de protecção e por fim deve ser realizada a formalização da política. As principais características de uma política são a precisão, a perceptibilidade, devendo esta explicar o motivo de ser utilizada e quem são os responsáveis pela mesma. Os procedimentos para a implementação da segurança são

[3] A Segurança da Informação nas Organizações feita com base em: MAMEDE, Henrique São - Segurança informática nas organizações. Lisboa: FCA - Editora de Informática, 2006. p.377-383

[4] Modelos e Políticas de Segurança nas Organizações feito com base em: MAMEDE, Henrique São - Segurança informática nas organizações. Lisboa: FCA - Editora de Informática, 2006. p.38-66

executados em partes: o objetivo, a descrição, as responsabilidades, a validade e a aprovação.

A Tecnologia da Informação (TI)

A inovação e o avanço tecnológico tem proporcionado grandes vantagens e impactos nas organizações devido aos primeiros contactos do homem com a máquina e a implantação da Tecnologia da Informação dentro das grandes, médias e pequenas empresas.

De acordo com Gonçalves (1993, apud PRATES; OSPINA, 2004 p. 14):

> A tecnologia é o fator individual de mudança de maior importância na transformação das empresas. Tais transformações não se restringem ao menos ao modo de produzir bens e serviços, mas induzem novos processos e instrumentos que atingem por completo a estrutura e o comportamento das organizações, repercutindo diretamente em sua gestão.

Importância da implementação de uma Política de Segurança numa Organização

A informação representa um recurso essencial numa organização. A perda de confidencialidade, integridade ou disponibilidade pode causar uma perda de confiança nos serviços que a empresa presta.[5] Actualmente, as organizações e os respectivos sistemas de informação e redes estão expostos a muitas ameaças relacionadas com a segurança. Os vírus, os hackers e outros ataques têm-se tornado cada vez mais difíceis de resolver. A informação é armazenada e transferida de diversas formas. Esta pode ser partilhada através do correio tradicional, correio electrónico ou outros meios informáticos, escrita em papel, etc. Esta informação deve ser protegida independentemente do seu suporte. Por isso, algumas medidas devem ser tomadas numa organização:

- A protecção da informação deve ser ajustada à sua importância e valor;
- Apenas o detentor da informação pode permitir o acesso à mesma;
- A segurança da informação deve ser tão importante como o cumprimento dos objectivos no seio de uma organização;

[5] Importância da implementação de uma Política de Segurança numa Organização feita com base em: Instituto de Informática – Carta de princípios de Segurança Informática e privacidade. [Em linha]. Lisboa : Ministério das Finanças, 2008. [Consult. 15 Novembro 2012]. Disponível em WWW: www.instinformatica.pt/o-instituto/instrumentos-gestao/seguranca-informatica-e-privacidade>

- A segurança da informação permite alcançar e manter um nível de qualidade elevado. Para isso, deve ser criada uma equipa de gestão da segurança da informação;
- A segurança da informação é um requisito essencial para o sucesso dos serviços de uma organização. Assim, todos os colaboradores ou pessoas que têm acesso à informação devem garantir a sua segurança e confidencialidade;
- É necessário adaptar de forma contínua as medidas de segurança de forma a acompanhar modificações tecnológicas e/ou sociais.

Gestão da Segurança da Informação (SI) na organização

Para muitas organizações, investir em tecnologia deixou de ser diferencial competitivo e passou a ser requisito para a permanência de sua organização no mercado. Então, buscar novas formas de inovação e novos parâmetros de organizar ou suprir todas as necessidades de uma empresa passou a ser fundamental nas tomadas de decisão dos líderes das empresas.

Gracioso (2002, p.12) ressalta que os líderes têm papel fundamental ao se obter uma Gestão de SI eficaz nas empresas, analisando que “esses executivos, pesquisadores e engenheiros são geralmente jovens, extremamente motivados e orgulhosos do trabalho que fazem .”.

Para se trabalhar com SIG, é preciso que os funcionários estejam preparados para utilizá-los da melhor maneira possível. Santos e Nascimento (2008, p.2) ressaltam a importância do treinamento do usuário aos programas de SGSI defendendo que:

> Isto se deve ao fato do usuário ser um ponto fraco para os casos de invasão de sistemas devido à falta de conhecimento das principais técnicas utilizadas pelos invasores. Prova disso é o sucesso dos ataques de spam, onde o usuário recebe um e-mail que o induz a executar um programa ou a acessar um site que coleta informações e as envia para algum invasor.

Portanto no SGSI é fundamental definir uma Política de Segurança, pois esta política formaliza os procedimentos para segurança da informação, que devem ser de conhecimento de todos. Estipulam-se normas, responsabilidades e punições para os que descumprirem as regras, além de obter um contrato de responsabilidades onde o funcionário confirma seu conhecimento a respeito das normas ali estabelecidas. De acordo com Rezende e Abreu (2010, p. 70):

A maneira mais moderna e efectiva de gestão de dados na empresa é a utilização das ferramentas dos Sistemas Gerenciadores de Banco de Dados (SGDB). Eles são recursos tecnológicos para trabalhos em banco de dados, transformando as bases de dados relacionais e únicas.

Princípios de Segurança

Para o processamento e armazenamento de informação em formato digital são utilizados os sistemas informáticos. Desta forma, os sistemas informáticos estão relacionados com a segurança de dados e da informação.[6]

Segundo Edward Waltz "os dados constituem observações individuais, medidas e primitivas de mensagens, estando na base da comunicação humana, das mensagens textuais, das interrogações electrónicas e nos instrumentos científicos de medição de fenómenos. A informação consiste em conjuntos organizados de dados, sendo que este processo organizacional pode incluir a ordenação, classificação, indexação e estabelecimento de relações, de forma a colocar os dados num determinado contexto para subsequente pesquisa e análise. A informação, uma vez analisada e compreendida, transforma-se em conhecimento." Os dados representam um fenómeno físico com o objectivo de desempenhar certos aspectos do nosso mundo real e conceptual. Estes são usados para difundir e depositar informação e para separar novas informações pela manipulação dos mesmos conforme regras formais definidas. À segurança informática acrescenta-se a dúvida em relação aos utilizadores sem sensibilidade para as questões que estão inteiramente relacionadas com a segurança, isto é, apesar destes possuírem requisitos de segurança não têm experiência nesta área. É a este problema que os profissionais em segurança informática devem dar resposta, identificando e desenvolvendo soluções que possibilitem respostas aos requisitos das organizações e dos utilizadores. Se o que pretendemos é a criação de sistemas que sejam seguros é necessária a utilização de mecanismos que protejam e permitam atingir os objectivos inicialmente propostos de forma a se conseguirem os níveis ambicionados.

A segurança tem a ver com o abrigo de bens, mas para isso estes têm de ser conhecidos, assim como o respectivo valor de cada um. É este conhecimento que nos possibilita a toma de diversos tipos de acção, designadamente:

[6] Princípios de Segurança feito com base em: MAMEDE, Henrique São - Segurança informática nas organizações. Lisboa: FCA - Editora de Informática, 2006. p.4-10

- **Prevenção:** determinação do valor de cada bem e dos riscos a que o mesmo está sujeito, na tentativa de os suprimir ou diminuir.
- **Detecção:** monitorização e acompanhamento persistentes que permitam estabelecer com precisão quando passou o incidente, como aconteceu e quem foi o culpado pelo mesmo.
- **Reacção:** acções que podem ser tomadas no sentido de restituir a situação antes do incidente, fazendo em simultâneo com que desapareça o risco de voltar a acontecer o mesmo. A segurança em sistemas informáticos, está relacionada com três aspectos principais:
- **Confidencialidade:** relacionada com a precaução da utilização não outorgada de informação.
- **Integridade**: relacionada com a premunição da alteração não outorgada da informação.
- **Disponibilidade:** relacionada com a precaução da retenção não outorgada de informação ou recursos. Não existe no entanto, uma definição unânime para a segurança de informação. Existem autores que adicionam outros itens à lista cuja ordem também é discutida, como por exemplo a autenticidade. A segurança de sistemas informáticos tem de garantir cinco princípios, designadamente:
- **Confidencialidade:** diz respeito ao estabelecimento de segredo, certificando que sempre que algo ou alguém não tenha licença, não possa tomar conhecimento de algo que está amparado.
- **Registo:** diz respeito à recolha de informação sobre o uso dos sistemas e seus recursos, garantindo a presença de dados para a execução de auditorias.

- **Fiabilidade e segurança**: dizem respeito à segurança de que os sistemas não introduzirão modificações a dados e que o uso dos recursos deixará sempre estes e os sistemas em estados intactos.

Dificuldades na Segurança Informática

Não existe uma definição exclusiva de segurança informática, mas sim linhas gerais que nos podem levar a um nível de implementação que seja o apropriado para o nosso caso em particular. Os problemas com a segurança estão relacionados com os

indivíduos com finalidades maliciosas. As ameaças aos dados provêm dos blackhats, dos crackers, dos hackers, dos script kiddies, entre outros [7].

Pré-condições para a segurança

A segurança de uma instituição deve ser estudada num teor alargado, tendo em conta diversos panoramas (dados, operações, aplicações, etc.). Devido a múltiplos assuntos relacionados com a segurança de uma organização deve-se tentar alinhar todos os aspectos que colaboram para a sua execução. Contudo, advoga-se muitas vezes à fixação desta abrangência, por parte daqueles que estão responsáveis pela segurança da instituição, que se fixam apenas nos temas ligados à segurança física, sendo o departamento da área de informática que define e promove as restantes medidas de segurança sem uma política que espelhe os preceitos de negócio nem os usos de auditorias. Assim sendo, acaba por não existir um plano exclusivo (integrado) de segurança. A ausência de um plano adaptado de segurança pode causar deficiências graves na instituição[8].

Identificação e Autentificação do Controlo de Acesso

Actualmente, é necessária a existência de segurança informática nas organizações, uma vez que protege o acesso não autorizado, ou seja, dá segurança aos dados para que estes não se encontrem acessíveis a quem não estiver autenticado para os consultar. Além do mais, é necessário proteger a informação em relação à sua utilização e modificação.8 É importante tentar definir o controlo de acesso, que se baseia na limitação do acesso aos recursos de um sistema auxiliando apenas os servidores. Para além disso, este controlo consiste em restringir o acesso físico a dispositivos de armazenamento de informação, entre outros. Salienta-se que os controlos de acesso podem dividir-se em duas partes tais como: controlos preventivos e controlos reactivos. No que diz respeito aos controlos preventivos, estes têm como finalidade evitar que os indivíduos que não fazem parte da entidade tenham acesso às instalações de hardware (documentação de sistemas). Já os controlos reactivos destinam-se a alertar os controlos de acesso físico que estão a ser invadidos (ex. sensores). Além dos controlos de acesso que foram mencionados, também existem outros como: controlos de recuperação (recuperam alguns recursos que deixaram de existir). É de grande importância afirmar que deve existir uma política de segurança nas entidades institucionais, pois essa política tem como objectivo

[7] Dificuldades na Segurança Informática feita com base em: MAMEDE, Henrique São - Segurança informática nas organizações. Lisboa: FCA - Editora de Informática, 2006. p.10-13

[8] Pré-condições para a segurança feita com base em: MAMEDE, Henrique São - Segurança informática nas organizações. Lisboa: FCA - Editora de Informática, 2006. p.13-16

descrever os requisitos num sistema e, sobretudo, proteger a informação existente nas instituições. Segundo Amoroso, o modelo de segurança constitui um meio de formalização de políticas de segurança. Esta formalização pode ser feita com base em dois paradigmas:

- O paradigma do controlo de acesso que consiste na existência de um sujeito passivo a tentar aceder a um recurso.
- O paradigma do controlo de fluxo de dados que tem como finalidade o controlo da informação que flui de um objecto para um sujeito passivo. Relativamente aos modos de acesso temos que ter em conta que se podem dividir em duas partes: o modo de observação (verifica o conteúdo do recurso, sem introduzir qualquer modificação) e o modo de alteração (possibilita qualquer alteração ao objecto). Já os direitos de acesso, têm como objectivo a definição de uma política de acesso. Os direitos de acesso com mais relevância são: Execute, Read, Append, Write.

Considerações finais

O presente trabalho tem como objectivos definir a implantação das técnicas de segurança de informação na inserção das novas como ferramentas de serviços e ter a melhor qualidade na vida prática das organizações, no que é concernente o tratamento das informações. E foi apresentado alguns princípios de seguranças de informações.

Referencias

ABNT NBR ISO/IEC 17799:2005 – Tecnologia da informação – Técnicas de segurança Código de prática para a gestão da segurança da informação, ABNT.

PRATES, Gláucia Aparecida; OSPINA, Marco Túlio. Tecnologia da Informação em Pequenas Empresas: Fatores de Êxito, Restrições e Benefícios. RAC – Revista de Administração Contemporânea, Rio de Janeiro, v. 8, n. 2, p. 9-26, abr./jun. 2004. ISNN 1415-6555.

REZENDE, Denis Alcides; ABREU, Aline França de. Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas. 7 ed. São Paulo: Atlas, 2010. ISBN 978-85-224-5993-3.

SANTOS, José Calisto dos; NASCIMENTO, A. D. do. Implantação de um Sistema de Gestão de Segurança da Informação na UFG. Goiânia, 2008. 6p. Artigo. Centro de Recursos Computacionais (CERCOMP). Universidade Federal de Goiás. 2008.