



Universidade Estadual Paulista

**Faculdade de Ciências
Campus de Bauru**

Artigo Científico: Segurança da Informação

Gustavo Dobkowski Longo

Artigo Científico apresentado na Disciplina de
Língua Portuguesa I
do curso de graduação
Bacharelado em Sistemas de Informação



SEGURANÇA DA INFORMAÇÃO

OBJETIVO

Apresentar aspectos gerais da segurança e legislação da informação.

PALAVRAS CHAVES:

- Segurança
- Informação
- Normas
- Legislação Pontual

RESUMO

Analisando nosso presente momento histórico, nos encontramos com um complexo e, de certo modo, eficiente mundo da informação. Entretanto como sendo complexo e quantitativo mostra-se , também com o decorrer do tempo e a evolução das tecnologias, altamente inseguro. As preocupações com segurança da informação torna-se cada vez mais primordiais, levando empresas, executivos e inclusive pessoas físicas a obterem conhecimentos no mínimo de conceitos básicos de segurança da informação.

Com o decorrer do tempo foram criados textos modelos e referências gerais para instruções e precauções básicas no ambiente tecnológico, com a evolução dessas atitudes criaram-se, através de órgãos e instituições públicas normas mais específicas, afim de padronizar o sistema de informação em geral.

Posteriormente e/ou paralelamente a esta fase de normatização, surgiu a elaboração e aplicação de modelos legislativos específicos aos sistemas de informação, levando em conta conceitos e modelos da segurança da informação.



INTRODUÇÃO

Esse artigo vem elucidar de forma clara e objetiva os aspectos gerais da segurança da informação. Nortear-se-a por quatro tópicos principais, os quais estão intrinsecamente ligados: considerações históricas da necessidade de proteção de informações trocadas; conceitos fundamentais e evolução da conscientização da proteção de informações; surgimento e evolução de *textos modelos* e normas principais; e surgimento, evolução e explanação da legislação competente a esse segmento.

Histórico e Normas

Desde o início da civilização humana há uma preocupação com as informações e com os conhecimentos atrelados a elas. Inicialmente, esta atenção especial pode ser observada no processo de escrita de alguns povos, como é o caso da antiga civilização egípcia, na qual somente as castas "superiores" da sociedade tinham acesso aos manuscritos da época, e menos pessoas ainda ao processo de escrita dos mesmos. Assim a escrita, por meio de hieroglifos do Egito antigo, representa uma das várias formas utilizadas pelos antigos de protegerem e, ao mesmo tempo, perpetuarem o seu conhecimento.

Contudo, somente na sociedade moderna, com o advento do surgimento dos primeiros computadores, houve uma maior atenção para a questão da segurança das informações. De início, esta preocupação era ainda muito rudimentar, porém com o passar do tempo este processo mudou.

A questão da segurança no âmbito dos computadores ganhou força com o surgimento das máquinas de tempo compartilhado (time-sharing), as quais permitiam que mais de uma pessoa, ou usuário, fizesse uso do computador ao mesmo tempo.

O time-sharing permitiu que vários usuários pudessem acessar as mesmas informações, contudo este acesso não gerenciado poderia gerar efeitos indesejáveis. Logo, nasce a necessidade da implementação de ferramentas que minimizem problemas de compartilhamento de recursos e informações de forma insegura.

Em outubro de 1967, nasceu nos Estados Unidos o primeiro esforço para solucionar tal situação. Isto se deu com a criação de uma "força tarefa", que resultou em um documento intitulado "Security Control for Computer System: Report of Defense Science Board Task Force on computer Security". Representou o início do processo oficial de criação de um conjunto de regras para segurança de computadores, que mais tarde chegaria ao seu cume com a publicação da uma norma internacional de segurança da informação no ano de 2000.



Porém, este esforço não se deu somente por parte do Departamento de Defesa dos Estados Unidos (United States Department of Defense – DoD), tendo o apoio da Agência Central de Inteligência (Central Intelligence Agency) que iniciou o desenvolvimento do primeiro Sistema Operacional que implementasse as políticas de segurança do DoD, que foi o ADEPT-50.

Em outubro de 1972, J. P. Anderson escreve um relatório técnico denominado: "Computer Security Technology Planning Study", no qual ele descreve de modo geral os problemas envolvidos no processo de se fornecer os mecanismos necessários para salvaguardar a segurança de computadores.

Este documento, combinado com os materiais produzidos por D.E. Bell e por L. J. La Padula, e denominados "Secure Computer Systems: Mathematical Foundations", "Mathematical Model" e "Refinement of Mathematical Model", deram origem ao que ficou conhecido como "Doctrine", esta por sua vez seria a base de vários trabalhos posteriores na área de segurança.

Paralelamente o Coronel Roger R. Schell, da Força Aérea americana, que na época trabalhava na Divisão de Sistemas Eletrônicos - EDS (Electronic System Division - Air Force Systems Command) iniciou o desenvolvimento de várias técnicas e experimentações que levariam ao surgimento do que ficou conhecido como "Security Kernels", que nada mais é do que os componentes principais para o desenvolvimento de um Sistema Operacional "Seguro".

Em 1977, o Departamento de Defesa dos Estados Unidos formulou um plano sistemático para tratar do Problema Clássico de Segurança, o qual daria origem ao "DoD Computer Security Initiative", que, por sua vez, desenvolveria a um "centro" para avaliar o quão seguro eram as soluções disponibilizadas.

A construção do "Centro" gerou a necessidade da criação de um conjunto de regras a serem utilizadas no processo de avaliação. Este conjunto de regras ficaria conhecido informalmente como "The Orange Book", e o Coronel Roger Shell foi o primeiro diretor deste centro.

O processo de escrita do "Orange Book", conhecido oficialmente como "Trusted Computer Evaluation Criteria - DoD 5200.28-STD", teve o seu início ainda no ano de 1978. No mesmo ano, a publicação da primeira versão "Draft", ou rascunho, deste manual, entretanto somente no dia 26 de dezembro de 1985 foi publicada a versão final e atual deste documento.

Graças às operações e ao processo de criação do Centro de Avaliação e do "Orange Book" foi possível a produção de uma larga quantidade de documentos técnicos, que representaram o primeiro passo na formação de uma norma coesa e completa sobre a segurança de computadores. A série de documentos originados pelo esforço conjunto dos membros do centro é reconhecida pelo nome de "The Rainbow Serie", cujos documentos continuam sendo atualizados largamente, tais documentos são distribuídos gratuitamente pela internet.

Mesmo que o "Orange Book" seja considerado, atualmente, um documento ultrapassado, podemos considerá-lo como o marco inicial de um processo mundial e contínuo de busca de um conjunto de medidas que permitam a um ambiente computacional ser qualificado como seguro.



Com a classificação realizada pelo "Centro" ficou mais fácil comparar as soluções fornecidas pela indústria, pelo mercado e pelo meio acadêmico de uma forma geral.

Outro fator a ser lembrado é que o "Orange Book", dentro de sua formalidade, permite, de uma maneira simples e coesa, especificar o que deve ser implementado e fornecido por um software, para que ele seja classificado em um dos níveis de segurança pré-estipulados, permitindo assim que este também seja utilizado como fonte de referência para o desenvolvimento de novas aplicações e para o processo de atualização ou refinamento de aplicações já existentes e em uso.

A existência de uma norma permite o usuário tomar conhecimento do quão protegidas e seguras estarão as suas informações, possibilitando ao mesmo uma ferramenta que irá auxiliar a escolha de uma solução. Do ponto de vista dos profissionais técnicos, eles passarão a possuir uma ferramenta comum de trabalho, evitando assim que cada equipe tenha para si um padrão desconexo das demais equipes, dificultando aos clientes a melhor escolha.

O "The Orange Book" representou o marco "zero", do qual nasceram vários padrões de segurança, cada qual com a sua filosofia e métodos proprietários, contudo visando uma padronização mundial. Houve um esforço para a construção de uma nova norma, mais atual e que não se detivesse somente na questão da segurança de computadores, mas sim na segurança de toda e qualquer forma de informação.

Este esforço foi liderado pela "International Organization for Standardization (ISO). No final do ano de 2000, o primeiro resultado desse esforço foi apresentado, que é a norma internacional de Segurança da Informação "ISO/IEC-17799:2000", a qual já possui uma versão aplicada aos países de língua portuguesa, denominada "NBR ISO/IEC-17799".

Características Pontuais

Dentro da área de segurança da informação lidamos com um conteúdo altamente técnico e conceitual, havendo assim a necessidade do conhecimento de diversas áreas e assuntos para uma compreensão e sucesso profissional aceitável. Abaixo cita-se pontualmente e concisamente boa parte desse conteúdo, tendo os termos agrupados conforme a correlação dos assuntos, e não em ordem alfabética:

- Ativo: Qualquer coisa que manipule direta ou indiretamente uma informação.
- Vulnerabilidade: Ponto pelo qual alguém pode ser atacado, molestado ou ter suas informações corrompidas.



- Ameaça: Algo que possa provocar danos à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de uma determinada vulnerabilidade.
- Risco: É medido pela probabilidade de uma ameaça acontecer e o dano potencial à empresa. Existem algumas maneiras de se classificar o grau de risco no mercado de segurança, mas de uma forma simples, poderíamos tratar como alto, médio e baixo risco.
- Confidencialidade: Não significa informação isolada ou inacessível a todos, mas sim a informação que deve ser acessada a quem lhe é de direito.
- Integridade: Diferente do que pode parecer, o conceito de integridade está ligado ao estado da informação no momento de sua geração e resgate. Ela estará íntegra se em tempo de resgate, estiver fiel ao estado original. A Integridade não se prende ao conteúdo, que pode estar errado, mas a variações e alterações entre o processo de geração e resgate.
- Disponibilidade: Este conceito tem despertado maior interesse depois que os negócios passaram a depender mais da informação para serem geridos. Afinal, de nada adiantará uma completa infra-estrutura tecnológica, com recursos que garantam a integridade e confidencialidade das informações, se quando por preciso acessá-la, a mesma não estiver disponível.
- Autenticidade: Defini-se pela veracidade do emissor e receptor de informações trocadas. Existem algumas tecnologias que permitem identificar os emissores e receptores de forma confiável, mesmo num lugar tão inócuo como o mundo virtual.
- Legalidade: Trata-se do embasamento legal as operações que se utilizam das tecnologias de informática e telecomunicação.
- C.I.D.A.L.: conceito base de segurança da informação, o qual congrega os cinco itens anteriormente citados: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.
- PCN (Plano de Continuidade de Negócios): Uma série de documentos que são elaborados com o propósito de se definir que ações serão tomadas em situações de crise e de emergência. Devem abordar desde a administração de crise, contingência operacional e recuperação à situação normal de funcionamento da empresa dentro do contexto do negócio do qual ela faz parte.



Legislação

A legislação competente à segurança da informação desenvolveu-se tendo como base os textos modelos e padrões normatizadores. Adotou-se as referências de normas já instituídas por Órgãos Oficiais, as quais criam o ambiente pertinente a aplicação da legislação, desta maneira há a possibilidade de adequação mais afinada dos modelos jurídicos à realidade do campo virtual.

A Internet trouxe um novo pensamento, um novo comportamento no cenário mundial. É o que segundo alguns juristas denominam de sociedade da informação, na qual existe reflexão da necessidade da existência de um marco jurídico que permita a livre circulação de bens e serviços, além de garantir a liberdade dos cidadãos.

Na União Européia (UE) várias batalhas estão sendo travadas para se atingir um denominador comum nas políticas de novas tecnologias de informação, a qual só pode ser assegurada por leis que permitam a regulamentação de cada país, a regulamentação entre empresas privadas e públicas e inclusive a regulamentação entre as pessoas físicas. Como a título de exemplo o Conselho da Europa apresentou a última versão de um documento sobre crimes virtuais, trata-se de um inventário com sanções penais e um dispositivo inspirado na legislação francesa.

Existe uma diretiva européia sobre o comércio eletrônico, a qual reconhece a assinatura digital, além da proteção de dados pessoais, está ganhando dimensão internacional num esforço para proteger o indivíduo.

Foi criada uma certificação digital comprovando que o usuário estava realmente praticando determinado ato com sua própria identidade. Trata-se de uma verificação feita em um banco de dados específico, com a aplicação da *Public Key Infrastructure* (PKI). Teve início em 1997 com conferências e iniciativas no comércio eletrônico através da *Organization for Economic Co-operation and Development* (OECD – Organização para Cooperação e Desenvolvimento Econômico e da *General Usage for International Digitally Ensured Commerce* (GUIDEC).

A utilização da chave pública obedece aos seguintes padrões internacionais: ISO 9796, ANSI X9.31, ITU-T x509, PACS, SWIFT.

Países que ainda estão criando as normatizações e legislações tendem a exigir tipos específicos de tecnologias para seguirem padrões já existente, desta maneira alcançam uma homogeneidade e compatibilidade com os demais países. Tomando-se tais atitudes, cria-se um ambiente propício a eliminação de obstáculos para que os certificados sejam reconhecidos em outras nações e as negociações possam ter realmente amparo judicial legal perante o comércio internacional.

De forma geral o mundo está consciente da real importância da elaboração de legislações específicas a tais ambientes e encontram-se tramites de projetos em diversos países, havendo de tal forma uma perspectiva altamente positiva para que num futuro breve tenhamos um sistema legislador específico e eficiente.



CONCLUSÃO

O tema segurança da informação mostra-se atualmente altamente abrangente, congregando diversas áreas da informática. Alia gestão e planejamento da informação, além de dispositivos sociais e tecnológicos, chegando inclusive ao âmbito da legislação.

Desta forma mostra-se extremamente complexo em um simples artigo conseguir abranger tudo, sendo assim, mostramos alguns tópicos e incitamos o leitor a buscar maiores informações para saciar sua sede de conhecimento neste assunto tão intrigante e interessante como a Segurança da Informação.

SOBRE O AUTOR:

Gustavo Dobkowski Longo é Diretor de Suporte e Hardware da empresa Firewalls, sendo conhecedor de Linux há dois anos e especialista em cabeamento estruturado, sendo integrador oficial dos produtos 3M (VIP – Volition Integrator Professional).

Para dúvidas, críticas e sugestões, contacte-o através do email: gustavo@firewalls.com.br.

Informações sobre a empresa Firewalls podem ser obtidas através do site: <http://www.firewalls.com.br>.

REFERÊNCIA BIBLIOGRÁFICA

<http://www.modulo.com.br>

<http://www.firewalls.com.br>

