Normas nacionais e internacionais de segurança da informação

Nesta aula serão abordados os principais aspectos envolvidos em Segurança e a história dos padrões e normas de Segurança da Informação que foram criados ao longo dos anos. Além disso, serão apresentadas algumas entidades nacionais e internacionais reconhecidamente aceitas como emissoras ou gestoras dessas normas.

A preocupação com relação à segurança de computadores não é um assunto novo, pois, desde a implantação dos sistemas operacionais de rede, houve a necessidade de colocar controles para saber o que estava sendo realizado por um determinado usuário ou aplicação do sistema.

Esse processo de segurança foi ao longo dos tempos tomando forma e implementando os controles necessários de acordo com as situações que iam acontecendo no cenário mundial das organizações.

Como informado na aula anterior, os ataques do dia 11 de setembro de 2001 mudaram de forma marcante a percepção das empresas com relação ao assunto segurança da informação, pois, após os ataques, deixaram de existir, não pelo fato de terem perdido os seus funcionários e suas instalações físicas, mas, sim, por não terem acesso a um ativo que naquele tempo não se tinha tanto controle, ou seja, a "informação".

Também nessa época a maioria dos incidentes de segurança era ocasionada por problemas relacionados a falhas da infraestrutura computacional e por isso muitos investimentos foram feitos buscando equilibrar essa dificuldade, e as organizações tinham de proteger os seus ativos físicos de TI. Não existiam equipes próprias para lidar com o assunto segurança da informação e por isso houve também a necessidade de treinamento dos funcionários nesse segmento.

Como um jogo de gato e rato, depois que as empresas resolveram os seus problemas com a infraestrutura, os problema de segurança migraram para os sistemas e aplicativos, que sofreram diversas técnicas sofisticadas de ataques e utilização de programas espiões, além de pichação de páginas de sites, roubo, alteração e manipulação indevida de dados da organização.

Nesse período também ficaram em evidência termos como: criptografia, autenticação, segregação de função, auditoria além da necessidade de segurança para os usuários e para os sistemas das organizações.

Normas de segurança em tecnologia da informação

O rápido crescimento das redes de computadores, e também da sua dependência, ocasionou

uma grande preocupação para as empresas, pois elas sentiram a necessidade de administrar/organizar as informações que trafegavam por meio das suas redes, bem como mantê-las em segurança.

Em um passado recente não existiam normas, nem padrões preestabelecidos que orientassem os procedimentos de segurança da informação dentro das corporações, porém esse cenário mudou muito nos últimos anos.

Com o surgimento de incidentes de segurança, foram criados ao redor do mundo vários procedimentos e normas para ajudar as empresas a proteger suas informações contra acessos indevidos e fraudulentos.

As normas

Uma norma pode ser vista como um documento que deve ser elaborado, aprovado e estabelecido por consenso por meio de uma autoridade reconhecida da organização, e pode ser utilizada para definir regras e padrões que servirão como um instrumento de controle na realização de alguma atividade de uso comum e repetitivo em certa situação.

As normas de segurança da informação foram criadas para fornecer as melhores práticas, diretrizes e princípios gerais para a implementação da gestão da segurança informação para qualquer organização.

Instituições padronizadoras reconhecidas

No mundo, existem algumas instituições nacionais e internacionais, reconhecidas como idôneas, que possuem a função básica de elaborar padrões e também de serem responsáveis pela edição, publicação e revisão das normas técnicas que serão seguidas por diversas áreas das organizações. Dentre essas organizações, podemos citar:

- **ISO** – International Standardization Organization.

- **IEC** – International Electrotechnical Comission.
- **ABNT** – Associação Brasileira de Normas Técnicas.

Logo no inicio, quando os computadores começaram a se conectar em redes, o controle de acesso físico era a principal preocupação das organizações. No Brasil, as primeiras orientações quanto à segurança física em informática foram definidas pelas normas técnicas NBRs.

- **NBR 1333**, de 12/1990 – Controle de acesso físico a CPDs (Centro de Processamento de Dados).
- **NBR 1334**, de 12/1990 – Critérios de segurança física para armazenamento de dados.
- **NBR 1335**, de 07/1991 – Segurança física de microcomputadores e terminais em estações de trabalho.
- **NBR 10842** – Equipamentos para tecnologia da informação e requisitos de segurança.

A seguir, vamos apresentar um breve histórico do surgimento das normas de segurança da informação ao redor do mundo.

Por volta do ano de 1967 nasceu nos Estados Unidos o primeiro esforço para tentar solucionar o problema da segurança em computadores, por meio da criação de uma "força tarefa" dentro do Departamento de Defesa (DoD – Department of Defense), que criou um documento intitulado "Security Control for Computer System".

Nesse mesmo momento foi criado um conjunto de regras que deveria ser utilizado nos processos que ajudariam os órgãos a efetuar a classificação dos sistemas operacionais como seguros ou não.

Esse conjunto de regras ficou conhecido informalmente como *The Orange Book* (O Livro Laranja), por causa da cor da capa que foi utilizada para o documento que continha essas regras.

Os níveis de segurança utilizados nesse livro seriam utilizados para avaliar e classificar o grau

de proteção que seria utilizado nos hardware, software e informações armazenadas nos sistemas de computadores.

Em seguida foi feita uma adaptação d?*O Livro Laranja* para poder englobar os aspectos de segurança relacionados não apenas aos computadores, mas também às redes de computadores.

Como esse documento foi escrito em outro documento que tinha a capa da cor vermelha, ele ficou conhecido como *Red book*.

Por volta do ano de 1989, o Departamento de Comércio e Indústria do Reino Unido criou um centro de segurança de informações cuja tarefa seria criar uma norma de segurança para o Reino Unido. Vários documentos preliminares foram publicados, até que, em 1995, surgiu a BS7799 (British Standard 7799).

Em virtude da sua complexidade e necessidade de segmentar os seus dois principais focos, esse documento foi dividido em duas partes designadas (BS7799-1 e BS7799-2):

A **BS7799-1 –** É a primeira parte da norma e foi feita como um documento de referência para implementar "boas práticas" para a segurança da informação.

A **BS7799-2 –** Segunda parte da norma, tinha como objetivo proporcionar uma base para a criação de um sistema de gestão da segurança da informação dentro das empresas.

Pelo fato de até aquele momento não existirem outros documentos que abordassem de forma estruturada esse tipo de assunto, esses documentos começaram a ser utilizados ao redor do mundo por diversas empresas que quisessem iniciar algumas ações relacionadas ao assunto Segurança da Informação. No entanto, como tinha diversos itens específicos e voltados ao país de origem, foi necessário que fosse modificado para a utilização de forma mundial.

A **ISO/IEC 17799:2000** é a versão internacional da BS7799, homologada pela ISO (International Standardization Organization).

A **NBR ISO/IEC 17799:2001** é a versão brasileira resultante da "tradução" da norma ISO, homologada pela ABNT em setembro de 2001, sendo que, em 2005, por conta do dinamismo da área de segurança, teve de sofrer uma série de revisões e tornou-se NBR ISO/IEC 17799:2005, publicada pela ABNT em agosto de 2005.

Outras normas

O processo de globalização, bem como a ocorrência de grandes fraudes financeiras em vários países, provocaram o surgimento de leis, normas, acordos e outras providências contábeis e financeiras que buscaram garantir a segurança de todos os envolvidos, entre os quais podemos citar:

LEI SARBANNES-OXLEY (SOX – SARBOX) – Legislação criada após os problemas apresentados nas contabilidades das empresas Enron e WorldCom, entre outras, e que afetava as empresas de comércio público dos Estados Unidos.

Tinha como objetivo dar transparência na divulgação das informações, assegurar a prestação de contas e tratar de forma justa e imparcial as partes interessadas.

BASEL II ACCORD (BASILEIA II) – Fornece uma diretriz para o cálculo de riscos (de crédito, do mercado e operacionais) de um banco e visa deixar mais eficiente os esforços de um banco para o gerenciamento dos seus riscos; no entanto, para conseguir isso é importante implantar com sucesso um programa de proteção das informações.

O PCI (PAYMENT CARD INDUSTRY) – Define um padrão para o manuseio de dados de pagamentos para todos os comerciantes e fornecedores de serviços que lidam com armazenamento, transmissão ou processamento de dados de cartões de crédito. Em caso de falha no cumprimento dos requerimentos do programa PCI ou na correção das vulnerabilidades existentes, pode resultar em uma série de dores de cabeça para a organização.

A ISO 15408 – Foi criada e direcionada para a segurança lógica das aplicações, bem como possui o foco principal no desenvolvimento de aplicações seguras. A ISO15408 define um método para avaliação da segurança de ambientes de desenvolvimento de sistemas.

ISO 27000 – Visando reunir as diversas normas existentes de segurança da informação, a ISO criou a série 27000, com normas específicas.

A norma ISO 27001:2005 é a norma BS7799-2:2002 revisada, com melhorias e adaptações, contemplando o ciclo de melhorias continua. As mudanças mais relevantes ocorreram na estrutura do sistema de gestão de segurança da informação (SGSI), quando foram destacados os aspectos de auditoria interna e indicadores de desempenho do sistema de gestão de segurança. Para facilitar e organizar o entendimento, essa norma foi subdividida em outras.

- **ISO 27002** – Trata-se do padrão que irá substituir a ISO 17799:2005.
- **ISO 27003** – Trata-se do novo padrão que abordará a gestão de risco.
- **ISO 27004** – Trata-se do padrão que abordará os mecanismos de mediação e relatórios para um sistema de gestão de segurança da informação (SGSI).

- **ISO 27005 –** Aborda itens e conceitos relacionados à implantação, monitorização e melhoria contínua do sistema de controles.
- **ISO 27006** – Está relacionada a itens que tratarão da recuperação e continuidade de negócio das organizações.

Além das normas citadas anteriormente, outras normas e padrões não tão específicos para a área de segurança de computadores indiretamente acabam ajudando nos processos internos que estavam sendo criados para garantir a segurança da informação, pois possuíam dentro dos seus escopos itens relacionados à segurança. Dentre eles podemos citar:

O ITIL (Information Technology Infrastructure Library) – È o modelo de referência para gerenciamento de processos de TI mais aceito mundialmente. Atualmente se tornou a norma BS-15000, sendo esta um anexo da ISO 9000:2000. Dentro dele existem itens específicos que abordam o assunto da Segurança da Informação, principalmente em planos de continuidade de negócios;

O COBIT (Control Objectives for Information and Related Technology) – É um guia de boas práticas apresentado como framework e mapas de auditoria, e um conjunto de ferramentas de implementação, bem como um guia com técnicas de gerenciamento.

A BS 25999-2 – É uma norma britânica criada em 2007 e tem como foco principal representar uma norma de gestão de continuidade de negócios. Define um sistema de gestão de continuidade de negócios que contém as fases de gestão (planejamento, implementação, análise e monitoramento), bem como a melhoria contínua.

A ISO 31000 (Gestão de Riscos) – Nova norma que foi criada para tratar de assuntos relacionados à gestão de riscos.

Para terminar, podemos afirmar que a evolução da Segurança da Informação acontece de forma constante, sendo assim, as normas, as leis e as regulamentações ligadas a essa área sempre estarão em processo de desenvolvimento, pois todos os dias novas vulnerabilidades e problemas de segurança são descobertos e há a necessidade da elaboração de novos procedimentos e mecanismos para poder combatê-los.

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento.
Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

Para memorizar os conhecimentos adquiridos nesta aula, clique no botão a seguir
e faça o caça-palavras proposto.

Clique no botão a seguir e teste sua memória e aprendizado entretendo-se com a cruzadinha.

A seguir, preencha a(s) lacuna(s) com a(s) palavra(s) adequada(s) às afirmações.

Referências

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de Segurança da Informação*: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. *Gerenciamento de Serviços de TI na Prática*: uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

SÊMOLA, Marcos. *Gestão da Segurança da Informação*: uma visão executiva. Rio de Janeiro: Elsevier, 2003.

WADLOW, Thomas A. *Segurança de Redes*: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2001.