Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

ABRAHÃO TOLENTINO SOARES DE FIGUEIREDO

PROSTA DE IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Brasília
2013

ABRAHÃO TOLENTINO SOARES DE FIGUEIREDO

PROSTA DE IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Redes de computadores de computadores com ênfase em segurança da informação

Orientador: Prof. Marco Antônio.

Brasília
2013

ABRAHÃO TOLENTINO SOARES DE FIGUEIREDO

PROSTA DE IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de computadores com ênfase em segurança da informação.

Orientador: Prof. Marco Antônio.

Brasília, ___ de _____ de 2013.

Banca Examinadora

_____

_____

RESUMO

Este trabalho apresenta uma proposta de planejamento, implantação e operação de um Sistema de Gestão da Segurança da Informação em uma organização. Para a elaboração dessa proposta foram analisados conceitos básicos de segurança da informação e métodos para a garantia da segurança. Também foram analisadas normas de segurança, como a ABNT NBR ISO/IEC 27001:2006 que define o que é um SGSI e dá diretrizes para sua implementação. A partir da análise desses temas foi elaborada uma proposta dividida em 11 etapas que estão inseridas nas quatro fases do ciclo PDCA. Os estudos realizados para a elaboração do método também podem servir de subsidio para a empresa durante a execução das etapas constantes na proposta, como na identificação de risco, classificação de ativos, seleção de controles de segurança, treinamento dos funcionários etc., ou seja, durante todo o processo de implantação do SGSI. Esse estudo dá orientações para qualquer tipo de organização que necessite implantar um SGSI ou melhorar um sistema já implantado.

Palavras-chave: Sistema de Gestão da Segurança da Informação. Tecnologia da Informação. Segurança da Informação. Normas ISO.

ABSTRACT

This document describes a method for planning, implementing and operating an Information Security Management System (ISMS). In order to be able to write this method we analyzed basic concepts of information security and ways to ensure the safety of information. Also were analyzed international standards, like ABNT NBR ISO/IEC 27001:2006 that defines what an ISMS is and gives directions on how to implement the system. The method described in this document is divided in 11 steps that are included in the PDCA cycle for continual improvement. The analysis that were made during the development of this document can help organizations during execution of the steps showed in the method, like for risk identification, assets classification, selection of security controls, staff training etc., it means during the execution of the whole method. This document gives orientation for any organization that is willing to implement an ISMS or improve one that is already installed.

Key words: Information Security Management System. ISO Standards. Information Technology. Information Security.

LISTA DE ABREVIATURAS E SIGLAS

ABNT: Associação Brasileira de Normas Técnicas

CERT.br: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

DES: Data Encryption Standard

ICP: Infraestrutura de Chaves Públicas

IDS: Intrusion Detection System

IEC: International Eletrotechnical Commission

IETF: Internet Engineering Task Force

IP: Internet Protocol

ISO: International Organization for Standardization

NBR: Norma Brasileira

PDCA: Plan, Do, Check, Act

RFC: Request for Comments

SGSI: Sistema de Gestão da Segurança da Informação

TI: Tecnologia da Informação

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

Vivemos em uma época de grande utilização da informação e a sua segurança tem se tornado um assunto muito importante para as organizações (SÊMOLA, 2003). Para suportar essa massiva utilização da informação, é necessário um gerenciamento e uma infraestrutura que suporte, de modo seguro e em tempo hábil, o grande volume de transações e armazenamento de dados.

Este trabalho se propõe a solucionar esse cenário demonstrando conceitos de segurança da informação, explicando o que pode dar errado (ataques e incidentes de segurança) e o que fazer para se prevenir (controles, normas, técnicas e ferramentas de segurança). Também traz um apanhado das principais normas internacionais que definem maneiras de gerenciar a segurança da informação na empresa.

Por fim o trabalho apresenta um método prático para a implantação das medidas definidas pelas normas apresentadas, permitindo estabelecer um SGSI que atende aos requisitos atuais de segurança da informação nas organizações.

Objetivo Geral

Propor uma metodologia para implantação de um sistema de gestão da segurança da informação em uma organização, com base em normas internacionais de segurança.

Objetivos Específicos

- Demonstrar conceitos básicos sobre segurança da informação;
- Analisar técnicas e ferramentas para garantia da segurança da informação;
- Analisar normas técnicas relacionadas à segurança da informação;
- Elaborar proposta para o planejamento e implantação de um sistema de gestão da segurança da informação em uma empresa, com base em padrões descritos em normas internacionais.

Justificativa

A constante manipulação de dados sigilosos nas organizações e a necessidade de se haver confiabilidade nos sistemas disponibilizados pelas empresas caracteriza a necessidade da existência de um sistema de gestão da segurança da informação (SGSI) que garanta que não haja perda de informações, que as informações estejam disponíveis sempre que necessário e que não aconteçam acessos indevidos. Este trabalho visa auxiliar na construção de uma metodologia para o planejamento, implantação e operação de um SGSI em uma organização, com base em uma série de padrões e normas internacionais de segurança da informação.

Metodologia

Este trabalho foi realizado com base em revisão bibliográfica e análise documental de temas relacionados à segurança da informação, normas e padrões da área.

O capítulo 2 traz conceitos básicos de segurança da informação, definição de risco, ameaça e vulnerabilidade, além de exemplos de incidentes de segurança. Também são apresentadas técnicas e ferramentas comuns que auxiliam no processo de garantia da segurança das informações nas empresas.

No capítulo 3 definimos o que é um sistema de gestão da segurança da informação e apresentamos normas de segurança que descrevem o funcionamento dos processos que compõem um SGSI.

No capítulo 4 é descrita uma proposta para o planejamento, implantação, operação e melhoria contínua de um SGSI, com base no ciclo PDCA, normas e padrões de segurança.

1 SEGURANÇA DA INFORMAÇÃO

Neste capítulo apresentaremos conceitos básicos de segurança da informação, definição de risco, ameaça e vulnerabilidade, além de exemplos de incidentes de segurança. Também serão apresentadas técnicas e ferramentas comuns que auxiliam no processo de garantia da segurança das informações nas empresas.

Atualmente as organizações têm se preocupado em proteger as suas informações contra ataques. Por outro lado a segurança da informação requer um investimento muito alto, que muitos gestores escolhem não fazer, por desconhecer todos os problemas que podem ocorrer devido à falta da implantação de um Sistema de Gestão de Segurança da Informação adequado.

A segurança da informação é um processo que visa proteger as informações de ameaças, levando em conta três objetivos fundamentais (BEAL, 2008):

- Integridade: é a garantia de que a informação não foi criada, alterada ou excluída por pessoas não autorizadas;
- Disponibilidade: é a garantia de que as informações estejam disponíveis sempre que solicitadas por pessoas autorizadas;
- Confidencialidade: é a garantia de que somente pessoas autorizadas tenham acesso à informação.

1.1 Risco

Riscos são considerados possibilidades de que ameaças utilizem vulnerabilidades de ativos para realizar ataques, causar danos, roubar ou destruir dados. Essas ações acarretam em prejuízos financeiros, por afetar os negócios da empresa, ou danos à imagem da organização (ABNT NBR ISO/IEC 27005:2008).

Segundo Michaelis “Risco é possibilidade de perigo, incerto, mas previsível, que ameaça de dano à pessoa ou a coisa...” (MICHAELIS, 2013), ou seja, é a possibilidade de um evento desfavorável ocorrer. É importante que os riscos sejam identificados para que seja possível atuar preventivamente para combatê-los. É possível ainda

apenas mapear, aceitar e monitorar os riscos, se o prejuízo que pode ser causado por ele for menor que o custo para evitá-lo.

1.2 Ameaça

Ameaças são agentes que podem explorar vulnerabilidades e causar incidentes que causam impactos aos negócios da organização (SÊMOLA, 2003). Os ativos estão expostos a ameaças, que podem provocar perdas de confidencialidade, integridade ou disponibilidade das informações.

As ameaças podem ser naturais, causadas por fenômenos da natureza; voluntárias, causadas por ações mal intencionadas; ou involuntárias, que são causadas por falta de treinamento, imprudência ou negligência de funcionários. Independente da origem da ameaça ela não deve ser ignorada.

Alguns exemplos de ameaças às informações são: enchente, terremoto, software mal intencionado, funcionários insatisfeitos ou mal treinados, furto e quebra de senhas, vazamento de informação.

1.3 Vulnerabilidade

Vulnerabilidade representa uma falha ou conjunto de falhas, é um elemento que pode ser explorado por uma ameaça e causar danos às informações e à organização (ALVES, 2006).

É uma fragilidade encontrada em um ativo que tem a possibilidade de ser utilizada por uma ameaça com o intuito de efetivar um ataque (BEAL, 2008).

As vulnerabilidades podem ser consideradas deficiências, que frequentemente não são identificadas a tempo ou, quando identificadas, não recebem o devido tratamento a fim de evitar o ataque (NAKAMURA; GEUS, 2002).

As suas origens podem ser diversas, como por exemplo: agentes da natureza; Falhar de hardware ou software; problemas nos meios de comunicação; ou ainda falhas humanas (SÊMOLA, 2003).

De acordo com a Norma ABNT NBR ISO/IEC 27002:2005 vulnerabilidade é a “fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças”.

Segundo Sêmola, vulnerabilidade é uma “brecha” ou janela que torna possível a ocorrência de uma ameaça (SÊMOLA, 2003), e para evitar a exposição dos ativos de uma organização a riscos é adequado rastrear e eliminar as vulnerabilidades. Ao identificar as vulnerabilidades, será possível dimensionar os riscos aos quais a organização está exposta e definir os controles de segurança mais apropriadas e prioritários para o tratamento desses riscos.

1.4 Incidentes

Quando as vulnerabilidades não recebem o tratamento adequado, de modo a corrigir falhas detectadas, incidentes de segurança podem se concretizar e causar grandes prejuízos.

Um dos passos necessários para se iniciar um plano de ação de segurança da informação é coletar informações de ocorrências de ataques e dos tipos de incidentes de segurança (HATCH; LEE; KURTZ, 2003).

O IETF (Internet Engineering Task Force) descreve, na RFC 2828, um ataque como sendo uma investida contra a segurança, um ato inteligente que tenta quebrar a segurança ou violar a política de um sistema. O ataque pode ser classificado como ativo quando altera recursos ou afeta a operação de um sistema, e como passivo quando tem acesso ou faz uso de informações do sistema sem afetar seus recursos.

O RFC 2828 classifica ainda um atacante como sendo interno ou externo. O atacante interno se trata de um usuário autorizado do sistema que o utiliza, de dentro do perímetro de segurança, de uma maneira não autorizada por aqueles que lhe

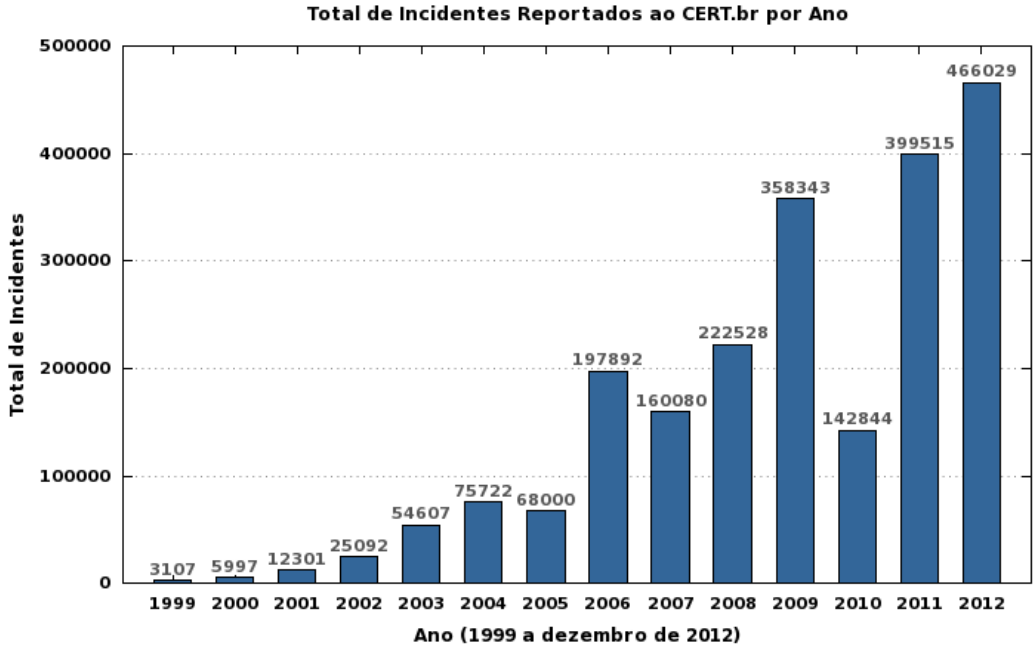
permitiram o acesso. Já o externo inicia o ataque de fora do perímetro de segurança e é um usuário não autorizado do sistema.

Técnicas comuns de ataques são: ataques a aplicações, que exploram vulnerabilidades do seu código; ataques a servidor web, normalmente de negação de serviço; SQL-Injection; cavalo de troia; vírus etc.

Há ainda a engenharia social, um tipo de ataque que normalmente não requer o uso de tecnologia. O atacante se utiliza do comportamento humano para burlar a segurança, sem que a vítima perceba sua real intenção. Funcionários, por ingenuidade e acreditando estarem sendo prestativas ou agindo com educação, fornecem informações importantes a pessoas mal intencionadas que as utilizam posteriormente para preparar um ataque contra a empresa (DAWEL, 2005).

Podemos observar no gráfico 1 o total anual de incidentes reportados por empresas situadas no Brasil ao CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, no período correspondente aos anos de 1999 a 2012. Observamos que há um aumento progressivo no número de incidentes, principalmente após o ano de 2006.

Gráfico 1 – Total de incidentes Reportados ao CERT.br por Ano.



Fonte: http://www.cert.br/stats/incidentes/ (acessado em 03/06/2013).

Conforme demonstrado no gráfico, podemos entender que apenas quantidade de ocorrências de incidentes de segurança já é uma grande motivação para as organizações pensarem em implantar um Sistema de Gestão de Segurança da Informação, visto que muitas informações são críticas. Algumas delas são secretas e possuem alto valor para a empresa. A implantação de um SGSI pode também auxiliar a empresa nas mudanças culturais e organizacionais relacionadas à segurança da informação.

1.5 Ferramentas

Ferramentas de segurança da informação são uma combinação de técnicas, hardwares e softwares, com objetivo de evitar e combater ataques (CHESWICK; BELLOVIN; RUBIN, 2005). Várias ferramentas são capazes de prover mais segurança quando são usadas em conjunto.

Alguns exemplos de ferramentas de segurança da informação são:

- Antivírus: são softwares projetados para detectar e eliminar vírus de computador, impedindo que arquivos suspeitos sejam executados. Para isso esses programas utilizam vários métodos para identificar um possível arquivo contaminado. Algumas formas de identificação de vírus usadas por esses softwares são: lista de vírus conhecidos, onde cada novo vírus descoberto é analisado e armazenado em uma lista; Análise heurística do código dos programas em execução; e análise de integridade do conteúdo dos arquivos salvos no computador.
- Firewall: É um tipo de software que tem o objetivo de não permitir a entrada de determinados pacotes IP na rede local, na tentativa de conter ameaças. Entre os tipos de firewall disponíveis podemos destacar: o filtro de pacote, que utiliza regras estáticas para filtrar pacotes que têm origem em servidores externos. (CHESWICK; BELLOVIN; RUBIN, 2005); o Proxy, que tem a finalidade de filtrar os pacotes que são gerados na rede interna da empresa e impedir a conexão com servidores externos que podem ser prejudiciais ao sistema; o firewall pessoal, um software que intercepta as conexões de entrada e saída em um computador de acordo com as

regras definidas pelo usuário; e o firewall reativo, que reconhece assinaturas de ataques e bloqueia o acesso indevido automaticamente.

- IDS: Os sistemas de detecção de intrusos ou Intrusion Detection Systems (IDS) funcionam em conjunto com o firewall e tem o objetivo de prover uma maior segurança na comunicação (ROESCH, 2006). Esses sistemas verificam o conteúdo de um pacote IP através de um sistema de assinaturas e, caso haja suspeição de violação da segurança, emitem um, permitindo que as configurações do firewall sejam aprimoradas daquele momento em diante. Formas comuns de uso dos IDS podem ser com base no computador (Host-Based) ou com base na rede (Network-Based). O IDS Host-Based monitora principalmente o log de eventos do micro em busca de comportamentos suspeitos, já o Network-Based monitora o tráfego na rede analisando o conteúdo dos pacotes IP.

1.6 Criptografia

É uma técnica utilizada para cifrar informações de forma que se tornem incompreensíveis para pessoas não autorizadas (KUROSE; ROSS, 2003).

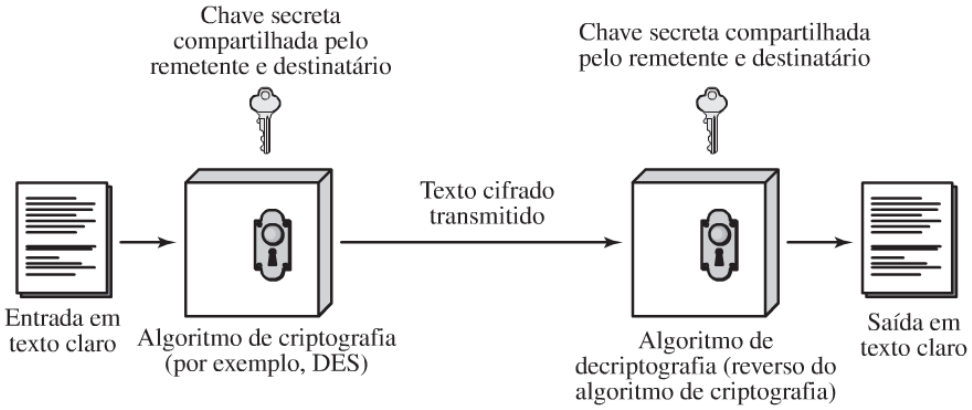
A criptografia tem sido usada historicamente principalmente por militares e diplomatas, entre outros. O texto a ser criptografado, chamado de texto simples (plaintext) é transformado, por meio de uma função matemática que utiliza uma chave criptográfica, que é um código secreto utilizado como um parâmetro para a função criptográfica. A saída desse processo é chamada de texto cifrado (cipher text) e transmitida ao destinatário da mensagem (TANENBAUM, 2011).

Existem duas classes de algoritmos de criptografia: os algoritmos de chave simétrica e os de chave assimétrica.

O algoritmo de criptografia simétrico, ilustrado pela figura 1, utiliza a mesma chave para codificação e decodificação de uma mensagem (TANENBAUM, 2011). Dessa forma, tanto o transmissor quanto o receptor da mensagem precisam conhecer a chave de criptografia utilizada para que possam cifrar ou decifrar a mensagem. O remetente usa a chave para criptografar e o receptor usa a mesma chave para

descriptografar, tornando difícil para quem não tem a chave de conseguir descobrir o conteúdo da mensagem. Um exemplo de algoritmo de criptografia simétrica é o DES (Data Encryption Standard), desenvolvido pela IBM, e que foi adotado pelo governo dos Estados Unidos em janeiro de 1977 para uso em produtos de segurança do setor de informática, porém já não é mais seguro em sua forma original.

Figura 1 – Modelo simplificado da criptografia convencional



Fonte: STALLINGS, 2008. p. 18.

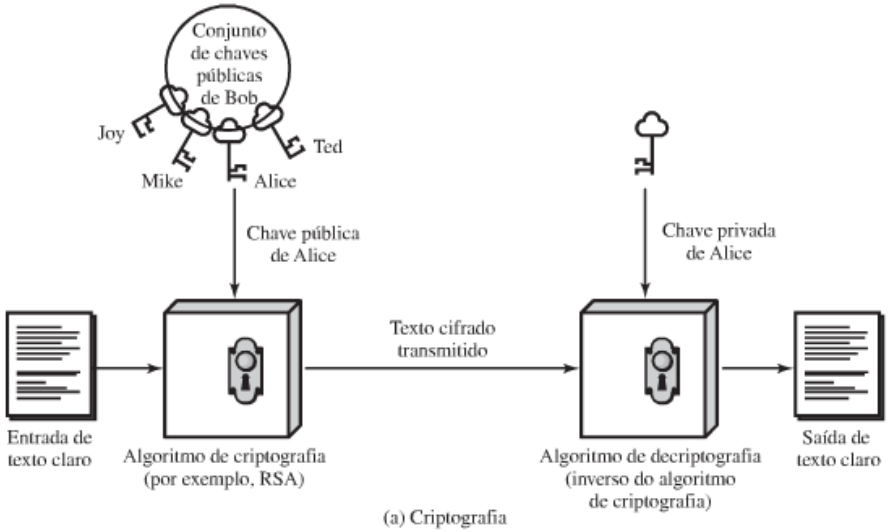
Nos algoritmos de chave simétrica um grande problema sempre foi a distribuição das chaves, já que se deveria pensar em uma maneira eficaz de transportar ou transmitir a chave criptográfica sem que intrusos tivessem acesso a ela, pois independente da robustez do algoritmo criptográfico, uma vez que uma pessoa estranha tinha o conhecimento da chave ela teria todas as condições para decifrar os textos cifrados transmitidos (TANENBAUM, 2011).

Com a intenção de resolver o problema da troca das chaves, os pesquisadores Diffie e Hellman da Universidade de Stanford propuseram um novo sistema de criptografia que utiliza chaves diferentes para criptografia e descriptografia (TANENBAUM, 2011).

Nesse sistema de criptografia cada usuário gera um par de chaves a ser usado para a criptografia e descriptografia das mensagens, eles então disponibilizam uma das chaves em um repositório de acesso público e mantêm a outra em segredo. Dessa

forma todos os participantes têm acesso às chaves públicas e as chaves privadas, que são geradas localmente, não precisam ser distribuídas (STALLINGS, 2008). A figura 2 demonstra como o sistema funciona.

Figura 2 – Criptografia de chave pública



Fonte: STALLINGS, 2008. p. 184.

1.7 Resumo de Mensagem

O resumo de mensagem ou função hash é uma função matemática que, aplicada a um texto gera um código de comprimento fixo chamado message digest (resumo de mensagem), esse código funciona como se fosse uma impressão digital do documento, já que é um código virtualmente único, que identifica o conteúdo do arquivo. O algoritmo é construído de uma forma que qualquer entrada gere uma saída sempre do mesmo tamanho e que não seja possível, a partir da saída, reconstruir o texto original. Ao aplicar em um arquivo a função hash é feito um cálculo para a geração de um código, com base no conteúdo do arquivo e qualquer alteração mínima do conteúdo do arquivo gera um resultado completamente diferente. Isso garante a integridade da informação, já que permite saber se o arquivo teve seu conteúdo alterado (STALLINGS, 2008). Algumas funções hash bastante conhecidas são o SHA-1, SHA-2 e MD5.

1.8 Assinatura Digital

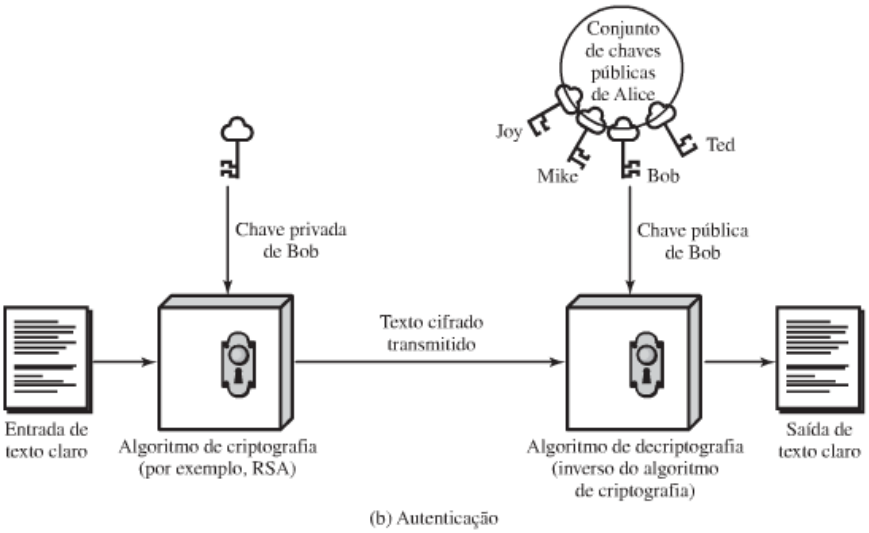
Em processos não informatizados, a assinatura manual é usada para determinar a autenticidade de muitos documentos (TANENBAUM, 2011). Já em sistemas computadorizados esse método não garante a autenticidade do documento digitalizado, por isso deve-se encontrar um meio de se realizar essa autenticação de um modo que não possa ser forjado.

A solução para o problema de se ter que substituir as assinaturas feitas à mão não é tão trivial, já que além da necessidade de se poder verificar a identidade do assinante, o transmissor não pode ser capaz de repudiar o conteúdo da mensagem, alegando desconhecer ou não ter sido de sua autoria. Outro cuidado que deve ser tomado é o de que o receptor não pode ser capaz de criar uma mensagem assinada por outra pessoa, sem que a pessoa realmente a tenha assinado.

O problema da assinatura digital foi resolvido hoje em dia se utilizando da combinação de duas técnicas: a criptografia de chave pública e o resumo de mensagem. Então para se assinar o documento é utilizada uma função hash, que gera o resumo da mensagem, e em seguida o resultado dessa operação, é criptografado utilizando a chave privada do assinante, dessa forma todos poderão descriptografar o resumo da mensagem, utilizando a chave pública do assinante, e comparar com um novo resumo gerado a partir da mensagem recebida. Dessa forma, se o resumo decifrado e o resumo gerado da mensagem recebida forem iguais, eles poderão ter certeza que a mensagem foi escrita por aquele remetente, já que somente ele possui a sua chave privada, usada para cifrar o resumo antes do envio (TANENBAUM, 2011). Dessa forma a assinatura digital garante a origem e a integridade da mensagem.

A figura 3 ilustra o funcionamento da assinatura digital utilizando a criptografia de chave pública, sendo que o texto de entrada corresponde ao resumo da mensagem (hash) a ser assinada.

Figura 3 – Assinatura digital



Fonte: STALLINGS, 2008. p. 184.

1.9 Autenticação

O serviço de autenticação tem o objetivo de garantir que uma comunicação é autêntica. Esse serviço tem funções de: garantir ao destinatário da mensagem que a mesma é proveniente de onde ela afirma ter vindo; garantir que, no momento do início da conexão, as entidades conectadas são autênticas, ou seja, que cada uma é a entidade que afirma ser; e, além disso, garantir que a conexão não sofra interferência de modo que um terceiro possa fingir ser uma das duas partes legítimas, e possa transmitir ou receber mensagens não autorizadas (STALLINGS, 2008).

A autenticação de mensagens é um conjunto de técnicas com o objetivo de se comprovar a identidade do usuário autorizado a acessar determinado recurso. Existem diferentes métodos de comprovação de identidade que podem ser utilizados na autenticação do usuário: baseado no que o usuário sabe, como por exemplo, senhas ou perguntas de segurança; baseado no que o usuário tem, como cartão, token ou crachá; ou ainda com base na biometria do usuário, como captura de impressão digital, analise da íris, da voz ou padrão de escrita etc. (NAKAMURA; GEUS, 2002).

Existem várias opções para realizar a identificação e autenticação do usuário, a empresa deve analisar e escolher o método mais adequado estratégica e financeiramente para a sua realidade. Vale lembrar que para se aumentar a segurança da autenticação podem ser utilizados vários métodos de identificação combinados para a realização de um único processo de autenticação, como identificação por cartão e senha ou impressão digital e token, entre outros.

2 SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Neste capítulo definimos o que é um sistema de gestão da segurança da informação (SGSI) e apresentamos normas de segurança que descrevem o funcionamento dos processos que compõem um SGSI.

Gestão de segurança da informação é um conjunto de medidas adotadas para implantação de controles que incluem políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, monitorados, analisados criticamente e melhorados, quando necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

Um Sistema de Gestão de Segurança da Informação (SGSI) segundo a Norma ABNT NBR ISO/IEC 27001:2006, envolve políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos da organização e é a parte do sistema global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Um dos objetivos do SGSI é impedir que uma ameaças identifique e explore vulnerabilidades do sistema e venham a causar danos a ele ou à empresa. Através da identificação desses pontos fracos, e do processo de gestão de risco, é possível agir preventivamente e aplicar, quando necessário, as medidas de segurança mais adequadas.

O SGSI é baseado no planejamento e aplicação de políticas de segurança, objetivos, diretrizes e normas, e tem como resultado a identificação e redução de riscos (Norma ABNT NBR ISO/IEC 27001:2006). Para implantar um SGSI é necessário devemos, primeiramente, definir seu escopo e localização geográfica e identificar as pessoas e processos que fazem parte da organização. Em seguida é realizado o levantamento dos ativos e mapeamento das vulnerabilidades e ameaças associadas a eles. Por fim é realizada a seleção dos controles que serão necessários para garantir a segurança desses ativos.

Um SGSI pode ser instituído na organização por um grupo multidisciplinar, com envolvimento da alta direção, através do estabelecimento de políticas de segurança, multiplicação do conhecimento entre os funcionários e determinação dos responsáveis e das medidas cabíveis, dentro dos limites de atuação de cada um, para a garantia da segurança das informações organizacionais. Dessa maneira, com a alta direção compromissada e com o treinamento eficaz dos colaboradores, é possível reduzir o número de ameaças que exploram eventuais vulnerabilidades.

Ao implantar um SGSI a organização também pode identificar vulnerabilidades e falhas de segurança dos sistemas, e propor correções que previnam ataques. Por esses motivos é essencial o apoio dos níveis estratégicos da organização. Outra questão fundamental é a implementação de um programa de treinamento para a conscientização dos usuários quanto à importância da Segurança da Informação para a empresa, tendo em vista que muitos processos e procedimentos de segurança definidos no SGSI serão realizados pelos usuários e caso haja desinteresse ou falta de conscientização, toda a segurança da empresa pode ficar comprometida. De acordo com vários especialistas a maior parte dos incidentes de segurança é causada por agentes internos, as estatísticas apontam que mais de 80% dos incidentes de roubo na internet são efetuados por eles (CERT). O sucesso da implantação de um Sistema de Gestão de Segurança da Informação depende também do apoio da alta direção da organização, e da dedicação e constante qualificação dos profissionais envolvidos.

2.1 Normas de Segurança da Informação

A preocupação com a segurança de sistemas informatizados é antiga. As primeiras definições de padrões e regras de segurança se deram na década de 60 (com o impulso da Guerra Fria), culminando com a publicação, no final do ano 2000, da norma Internacional de Segurança da Informação ISO/IEC 17799, que teve nova edição publicada em 2005 como ABNT NBR ISO/IEC 27002:2005, já com o novo esquema de numeração.

A ISO “International Organization for Standardization” é uma organização com sede na Suíça e tem como função desenvolver e promover normas que possam ser utilizadas igualmente em todos os países (ABNT NBR ISO/IEC 27001:2006). A Sigla ISO foi originada da palavra Isonomia. O Brasil é representado pela Associação Brasileira de Normas Técnicas - ABNT.

2.1.1 A Norma ABNT NBR ISO/IEC 27002:2005

A norma ISO/IEC 17799 teve sua origem no final da década de 80. Em 1987, no Reino Unido, o Department of Trade Centre (DTI) criou o Comercial Computer Security Centre (CCSC) que tinha o objetivo de definir critérios para avaliação da segurança e dessa forma auxiliar companhias britânicas que comercializavam produtos para segurança de Tecnologia da Informação.

Além disso, o CCSC criou um código de segurança para os usuários das informações denominado PD0003 – Código para Gerenciamento da Segurança da Informação, em 1989. Desde então esse centro publicou vários outros documentos preliminares até que, em 1995, surgiu a norma BS7799.

Essa norma foi dividida em duas partes, a primeira, publicada em 1995 e a segunda em 1998. Em dezembro de 2000, após incluir várias alterações e sugestões, a primeira parte da BS7799 se tornou uma norma internacional com sua publicação na forma da ISO/IEC 17799. Em 2005 ela passou a se chamar ABNT NBR ISO/IEC 27002:2005 após uma atualização.

Ela pode ser utilizada como um documento de referência ou guia de melhores práticas, estabelece diretrizes e princípios gerais para a gestão de segurança da informação, e contém uma lista de controles com o objetivo de garantir a segurança da informação, além de várias orientações para sua gestão nas organizações (ABNT NBR ISO/IEC 27002:2005).

É apontado na norma que a garantia da segurança da informação significa: proteger a informação de ameaças, de forma que seja possível a continuidade dos negócios; diminuir os riscos de segurança e consecutivas perdas, de modo a

maximizar os lucros; e melhorar as oportunidades de negócio, por meio da manutenção da imagem da empresa.

Os principais requisitos da ABNT NBR ISO/IEC 27002:2005 são apresentados no Quadro 1.

Quadro 1 – Requisitos da Norma ABNT NBR ISO/IEC 27002:2005.

Requisito	Descrição
Política de segurança	São normas desenvolvidas que consideram as responsabilidades, punições e autoridades.
Segurança organizacional	Estrutura da gerência de segurança
Classificação e controle de ativos de informação	Classificação, registro e controle dos ativos.
Segurança relacionada às pessoas	Foco do risco decorrente de ações das pessoas
Segurança ambiental e física	Levantamento da necessidade de definição das áreas de circulação restrita e de se proteger equipamentos e infraestrutura de TI
Gerenciamento das operações e comunicações	Aborda temas relacionados a procedimentos operacionais, homologação de sistemas, entre outros
Controle de acesso	Controle de acesso aos sistemas, definição de competências e responsabilidades.
Desenvolvimento e manutenção de sistemas	Requisitos para sistemas, criptografia, arquivos, desenvolvimento e suporte de sistemas.
Gestão de incidentes de segurança	Notificação de vulnerabilidades, ocorrências de segurança e gestão de incidentes.

Gestão da continuidade do negócio	Reforço na necessidade de ter um plano de continuidade e contingência

Fonte: Adaptado de (ABNT NBR ISO/IEC 27002:2005).

Ela está dividida em 16 capítulos, abaixo o detalhamento dos principais capítulos que compõem a norma:

- Análise, avaliação e tratamento de Riscos: a norma indica que as análises e avaliações de risco devem identificar e priorizar os riscos a partir de critérios de aceitação dos riscos e dos objetivos definidos pela organização.
- Política de segurança: esse capítulo define o que é a Política de Segurança da Informação. Ela é um documento de alto nível que orienta ações e implementações futuras e é utilizada em conjunto com outros documentos como normas e procedimentos, que abordam detalhamentos sobre os padrões e procedimentos de segurança a serem aplicados (NAKAMURA; GEUS, 2003).
- Segurança organizacional: Aborda a estrutura de uma gerência para segurança da informação, define as responsabilidades dos usuários pela segurança da informação, incluindo agentes externos e fornecedores de serviços.
- Classificação e controle dos ativos de informação: Define a classificação, o registro e o controle das informações da organização.
- Segurança em pessoas: indica como diminuir os riscos de falha humana, roubo, fraude ou uso impróprio das instalações, através da conscientização dos usuários, de acordo com seus cargos, sobre as ameaças à segurança da informação organizacional.
- Segurança ambiental e física: Segurança das áreas de circulação restrita e a necessidade de se protegerem os equipamentos e a infraestrutura de TI da empresa.
- Gerenciamento das operações e comunicações: Aborda as principais áreas físicas e operacionais que devem ser objeto de especial atenção da segurança. Dentre estas áreas destacam-se: procedimentos operacionais e respectivas responsabilidades, homologação e implementação de sistemas, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda

de cópias de segurança, controle de documentação, segurança de correio eletrônico etc.

- Controle de acesso: indica métodos para controlar o acesso à informação, prevenir o acesso não autorizado a sistemas, equipamentos e rede.
- Desenvolvimento de sistemas e manutenção: Aborda os requisitos de segurança dos sistemas, desenvolvimento, dados e suporte, garantindo a confidencialidade, autenticidade e integridade da informação, assegurando que projetos de tecnologia da informação e suporte de atividades sejam conduzidos de maneira segura.
- Gestão de continuidade do negócio: Previne para que não ocorram interrupções nas atividades e processos críticos do negócio devido às falhas e desastres, reforça a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e atualizado.
- Conformidade: Evita que a organização viole leis civis ou criminais, obrigações legais ou contratuais, ou segurança de sistemas e informações de terceiros. Também visa a maximizar a efetividade e minimizar a interferência em sistema de auditagem.

Ao todo a norma contempla 127 controles, mas vale lembrar que o uso de todos nem sempre é necessário para se garantir um bom nível de segurança. Esses controles devem ser selecionados de acordo com a análise de risco realizada na empresa. A integração com outras normas e padrões também é de grande valia nesse processo.

2.1.2 A Norma ABNT NBR ISO/IEC 27001:2006

A norma ABNT NBR ISO/IEC 27001:2006 foi baseada na segunda parte da norma BS7799, ela define requisitos para que a organização possa estruturar um sistema de gestão de segurança da informação (SGSI), além de um processo de avaliação de risco e classificação de ativos, ajudando na análise e identificação dos riscos e na implantação de controles para minimizá-los (ABNT NBR ISO/IEC 27001, 2006).

No Quadro 2 apresentam-se os requisitos existentes na norma ABNT NBR ISO/IEC 27001:2006.

Quadro 2 – Requisitos da Norma ABNT NBR ISO/IEC 27001:2006.

Número	Requisito	Descrição
1	Escopo	Abrangência da Norma
2	Referência Normativa	Normas e padrões relacionados à norma 27001
3	Termos e Definições	Termos e definições relacionados à segurança da informação
4	Sistema de Gestão da Segurança da Informação	Referente à criação, implementação, monitoramento e melhoria do SGSI, também trata de documentação e registros de informações.
5	Responsabilidade da Direção	Definição de responsabilidades, treinamento e provisão de recursos do SGSI.
6	Auditorias Internas	Auditorias Internas realizadas por pessoal treinado e comprometido com o SGSI
7	Analise crítica do SGSI	Análise realizada pelo corpo diretivo da organização das ações efetuadas pelo SGSI
8	Melhoria do SGSI	Trata das ações corretivas e preventivas efetuadas pelo SGSI

Fonte: Adaptado de ABNT NBR ISO/IEC 27001:2006.

Um SGSI é um sistema de gestão similar a um Sistema da Qualidade e também passível de certificação. Para a certificação são analisados um conjunto de documentos, práticas e procedimentos que evidenciam a implantação de controles constantes na norma, e que devem ser continuamente executados e devidamente registrados. Este modelo de gestão está baseado no ciclo com melhoria contínua PDCA (Plan-Do-Check-Act).

Criado em 1920, o ciclo PDCA é indicado na norma como um meio para facilitar o gerenciamento dos processos do SGSI. No modelo as atividades iniciais são as de

planejamento, na fase "Plan", passando para as de execução, na fase "Do", as de monitoramento, na fase "Check", e por último as atividades de melhoria, na fase "Act". Esse ciclo é repetido sucessivamente enquanto o sistema estiver em operação, para que a cada novo ciclo, o sistema seja melhorado.

A Norma ABNT NBR ISO/IEC 27001:2006 utiliza o PDCA para propor as fases da gestão da segurança da informação. Seguindo as etapas definidas no modelo podemos implementar, de forma planejada, um SGSI que objetiva a minimização e eliminação dos riscos. (ABNT NBR ISO/IEC 27005:2008). Ao seguir as definições do PDCA podemos constatar, por exemplo, que a Análise de Riscos da Organização, onde é feita a análise e classificação dos ativos, deve ser realizada antes da implementação do Plano de Continuidade de Negócios.

As duas primeiras fases do PDCA (Planejar e Fazer) do PDCA correspondem às etapas de estabelecimento, implementação e operação do SGSI, que inclui: definição do escopo e do que está fora do escopo; elaboração da política de segurança; realização da análise de risco; definição de uma estratégia para a gestão dos riscos; e seleção e documentação dos controles necessários para reduzir os riscos identificados.

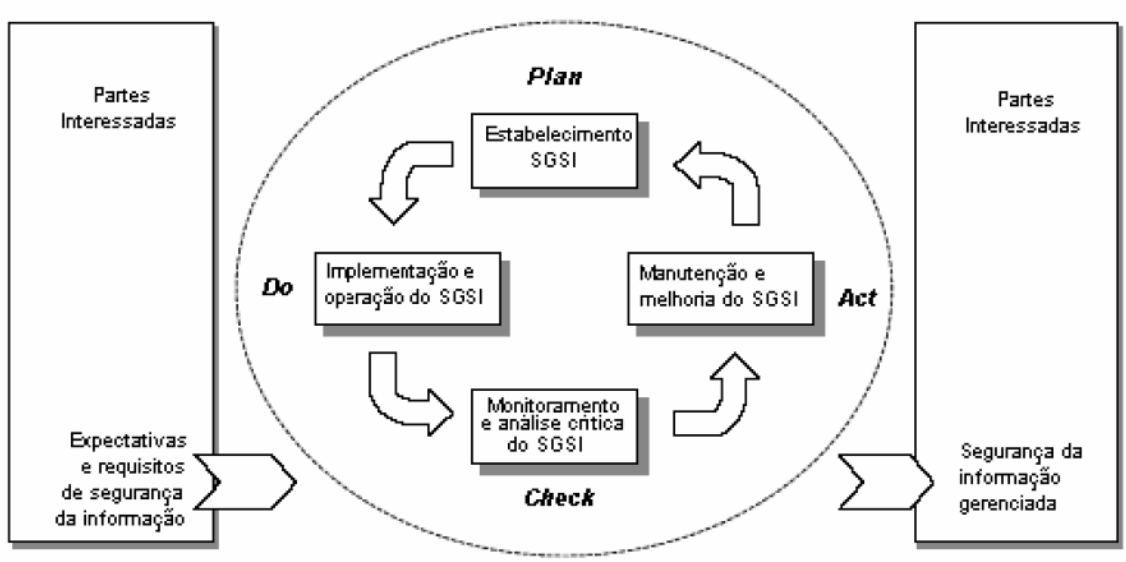
Ou seja, todas as atividades de planejamento e implantação do sistema ocorrem nessas duas primeiras fases do PDCA, é quando deverão ser definidos os limites para implantação do SGSI, o escopo e os ativos que deverão ser protegidos, indicando os responsáveis, as vulnerabilidades e ameaças associadas. Já que só é possível selecionar os controles e eliminar os riscos após essas definições. É bom notar que nesses momentos de decisão deve haver a participação da alta direção da empresa.

As duas últimas fases (Verificar e Agir) correspondem à: verificação do cumprimento das medidas de segurança especificadas nas fases anteriores; verificação das soluções de segurança utilizadas; melhoria contínua do sistema; e auditorias periódicas dos componentes do sistema. Esse é o momento quando o responsável pela Segurança da Informação, com autorização da direção da empresa, avalia se as ações propostas anteriormente estão sendo realizadas e, havendo

divergência com o planejamento, deve atualizar os procedimentos ou aplicar as correções necessárias, com o objetivo de melhorar continuamente o SGSI.

A Figura 4 ilustra o modelo PDCA e ações referentes a cada fase para atendimento aos requisitos de segurança de informação.

Figura 4 – Modelo PDCA aplicado aos processos de SGSI.



Fonte: Norma ABNT NBR ISO/IEC 27001:2006.

Um bom Sistema de Gestão de Segurança da Informação tem por objetivo prover uma orientação e apoio à direção para a segurança da informação de acordo com os requisitos do negócio e com as Leis e regulamentações relevantes. Através do SGSI será possível identificar as áreas de atuação que merecem mais atenção, podendo aplicar correções de forma objetiva e transparente para toda a organização.

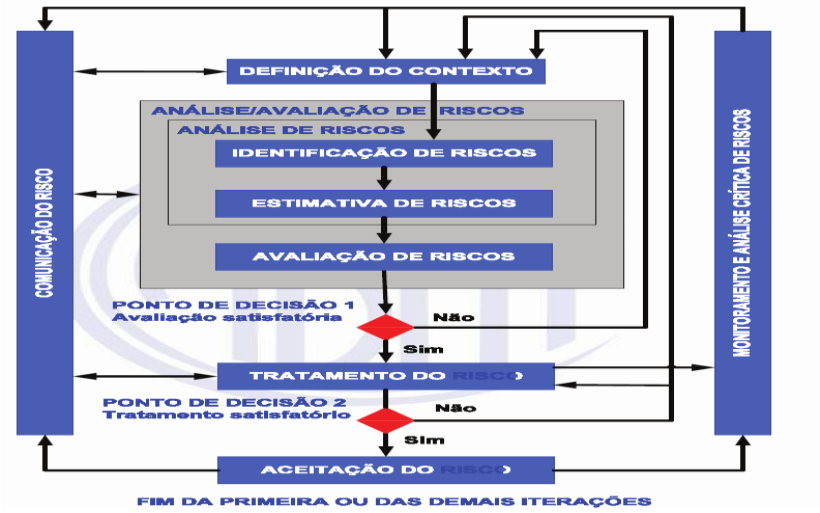
2.1.3 A Norma ABNT NBR ISO/IEC 27005:2008

A Norma ABNT NBR ISO/IEC 27005:2008 é o documento que auxilia o Gestor de Segurança da Informação no processo de gestão de riscos e contém sua descrição. Segundo a Norma o processo de Gestão de Risco consiste em:

- Definição do Contexto – é uma análise da organização definindo suas principais características, o escopo e os limites de atuação;
- Análise e Avaliação de riscos – nesta etapa os riscos são identificados e classificados conforme sua ordem de prioridade e relevância;
- Tratamento do Risco – é a etapa onde os controles para reduzir, evitar ou transferir os riscos são definidos (Plano de Tratamento de Risco);
- Aceitação do Risco – esta etapa consiste na aceitação do risco, pois se não há possibilidade de evitar ou tratar o risco, ou se o investimento for maior que o possível prejuízo que o risco pode causar, é importante aceitá-lo e registrar a decisão identificando o responsável pela decisão;
- Comunicação do Risco – é a etapa onde as informações sobre o risco devem ser disseminadas para todos os envolvidos;
- Monitoramento e Análise Crítica de Riscos – etapa em que os riscos e seus fatores são monitorados criticamente, a fim de agir com maior agilidade nas possíveis mudanças no contexto da organização.

Para melhor visualizar, a Figura 5 apresenta etapas do processo de Gestão de Risco. O processo é iniciado com a Definição do Contexto, então é feita a análise e avaliação dos riscos, seguida das etapas de tratamento e aceitação do risco. As etapas de comunicação do risco e de monitoramento e análise crítica são executadas durante todo o processo de gestão do risco.

Figura 5 – Processo de Gestão de Riscos de Segurança da Informação.



Fonte: Norma ABNT NBR ISO/IEC 27005:2008.

No Ponto de Decisão 1 (Figura 5), após a análise e avaliação dos riscos, é verificado se a avaliação foi satisfatória, se afirmativo a etapa está cumprida, devendo partir para o Tratamento do Risco, caso negativo o processo retorna para a Definição do Contexto. O mesmo ocorre no ponto de decisão 2 que, caso o tratamento dos ricos não tenha sido satisfatório, o processo retorna para o início.

A etapa de Aceitação do Risco consiste em explicitar de forma transparente todos os riscos existentes, por exemplo, nos casos onde a implementação de uma ação é postergada pela escassez de recursos financeiros, é interessante que fique claro todos os riscos que o adiamento daquela implementação vai acarretar.

No processo de Gestão de Riscos é importante efetuar em todas as etapas a comunicação dos riscos existentes para o pessoal operacional e os gestores da organização. A conscientização do pessoal sobre todo o processo ajuda no momento de lidar com os incidentes e eventos não previstos de forma mais efetiva.

As atividades da etapa de Monitoramento e Análise Crítica dos Riscos são constantes, pois os riscos não são estáticos e precisam de monitoramento contínuo. Por exemplo, caso a organização adquira novos ativos, estes devem ser incluídos no monitoramento.

3 PROPOSTA DE IMPLANTAÇÃO DO SGSI

Neste capítulo apresentaremos uma proposta de implantação de um SGSI em uma empresa, com base no estudo das normas de segurança da informação. O escopo deste trabalho não inclui os detalhes técnicos necessários para atender necessidades específicas de uma organização, porém o estudo pode ser utilizado por empresas como referência para a construção de um sistema gestão da segurança da informação personalizado para a sua realidade.

A proposta de implantação do SGSI é dividida em 11 etapas, que serão detalhadas no decorrer desse capítulo. A primeira etapa se refere ao planejamento inicial e é executada apenas uma vez, antes de se iniciar o processo de implantação. As outras 10 etapas são executadas seguindo o ciclo PDCA para melhoria contínua.

As etapas de definição do escopo, elaboração da política de segurança, identificação e classificação de ativos, análise e identificação de riscos, e planejamento da gestão de risco, correspondem ao estabelecimento do SGSI e são realizadas durante a fase de planejamento (plan) no ciclo PDCA proposto na ABNT NBR ISO/IEC 27001:2006. Na fase de implementação e operação do SGSI, no PDCA, também chamada de “fazer” (do), são executadas as seguintes etapas da proposta: implementação da estratégia de gestão de risco; elaboração da declaração de aplicabilidade; e de treinamento e conscientização dos funcionários. Já as etapas de monitoramento e análise e de manutenção e melhoria correspondem, respectivamente, às fases verificar (check) e agir (act) do PDCA.

3.1 Planejamento Inicial

Inicialmente deve-se fazer um planejamento do sistema. É uma etapa que acontece antes do início da construção do sistema e engloba: o estudo de viabilidade do projeto; estimativas de custo e de alocação de pessoal; e definição de cronograma, objetivos e metas.

Essa fase é realizada normalmente em duas etapas. Na primeira realiza-se um diagnóstico da situação atual, onde é verificada a existência de controles e políticas

já implementados. Na segunda é realizado o planejamento do SGSI e a preparação para a sua implantação.

A norma ABNT NBR ISO/IEC 27001:2006 recomenda a formação de um comitê responsável pela implantação do Sistema na organização. Os principais papéis deste grupo são: promover a conscientização dos funcionários; planejar e preparar o sistema; definir a política de Segurança da Informação da empresa; e estabelecer, de acordo com o planejamento estratégico da organização, os objetivos e metas para o Programa de Gerenciamento da Segurança da Informação.

3.2 Definição do Escopo

A definição do escopo, de acordo com a norma ABNT NBR ISO/IEC 27001:2006, deve ser feita levando em consideração as características do negócio, da organização, de sua localização, seus ativos e tecnologias. A declaração do escopo deve conter: uma descrição da organização, do seu negócio e sua localização geográfica; processos de negócio e sistemas de informação incluídos no escopo; plantas do edifício, leiautes e diagramas de rede; além das justificativas para exclusões do escopo. Todo o projeto e suas futuras revisões terão como base essa definição de escopo. A delimitação do escopo é extremamente importante, pois quanto maior o escopo maior a complexidade do SGSI a ser implementado.

A norma ABNT NBR ISO/IEC 27005:2008 descreve requisitos que funcionam como subsidio para a escolha do escopo, são eles: os objetivos estratégicos da organização; seus processos de negócio; suas funções e estruturas; requisitos legais, regulatórios e contratuais aplicáveis à organização; a política de segurança da informação; seus os ativos; suas localidades e características geográficas; restrições e expectativas; ambiente sociocultural; e interfaces.

3.3 Elaboração da Política de Segurança da Informação

A tarefa de definição, revisão e atualização da política de segurança da organização é realizada pelo comitê responsável pela gestão da segurança da

informação e deve ter como base os padrões e normas apresentados anteriormente nesse trabalho.

A Política de Segurança é uma demonstração do comprometimento da gerência com a segurança da informação na empresa, é um documento que descreve as recomendações gerais, regras, responsabilidades e práticas de segurança. Ela deve ser moldada às características e necessidades específicas de cada organização e necessita ser constantemente monitorada, revisada e atualizada. É fundamental que a política de segurança seja efetivamente utilizada como referência pelos funcionários da empresa, para que seja possível garantir os três princípios básicos da segurança da informação: integridade, disponibilidade e confiabilidade. Vale lembrar que os seus resultados normalmente só poderão ser notados a médio e longo prazo.

A Norma ABNT NBR ISO/IEC 27002:2005 recomenda que a Política de Segurança apresente as seguintes características: tenha sido aprovada pela alta direção, divulgada e publicada de forma ampla para todos os colaboradores; seja revisada regularmente; esteja em conformidade com a legislação e cláusulas contratuais; defina responsabilidades gerais e específicas; e disponha as consequências de eventuais violações.

Além destas características a política de segurança deverá abranger os seguintes tópicos:

- Propriedade da Informação – quem é o responsável pela informação, a pessoa que pode definir quem deverá ter acesso a determinadas informações e em qual nível de acesso. O responsável pela informação também deve ser consultado na criação da política de backup.
- Classificação da informação – o gestor deverá classificar a informação quantos aos princípios de disponibilidade, confidencialidade e integridade.
- Controle de acesso – devem ser documentados todos os pedidos de acesso. Deve haver separação de função, de modo que um mesmo usuário não seja responsável, por exemplo, por realizar um pedido e autoriza-lo. É importante, também, que se mantenham as trilhas de auditoria no sistema.

- Gerência de Usuários e Senhas – as senhas devem ser individuais. Deve haver política que garanta senha forte e com trocas periódicas. É importante explicitar que a responsabilidade pela senha é do usuário. Deve ser definido um efetivo gerenciamento das contas de usuários do sistema, de preferência com integração com o setor de recursos humanos.
- Segurança Física – acessos às áreas restritas devem ser controlados quanto à entrada e saída de pessoas e equipamentos. Toda concessão de acesso deve ser registrada. Também é importante a realização de auditorias periódicas.
- Desenvolvimento de sistemas ou compra de software – é importante a definição de um processo de desenvolvimento que proponha requisitos de segurança. Softwares comprados devem ser analisados quanto ao cumprimento dos requisitos de segurança definidos pela organização.
- Plano de continuidade de Negócios – devem ser definidos controles e padrões que especifiquem os detalhes do plano de contingência e continuidade dos negócios.

Vale ressaltar que as políticas criadas devem ser seguidas por todos os colaboradores da empresa e devem servir como referência e guia de segurança da informação. Para isto, é necessária a realização de uma campanha de divulgação e conscientização de sua importância para a organização.

Quadro 3 – Exemplo simples de uma política de segurança da informação:

EMPRESA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO

A Política de segurança da informação aplica-se a todos os funcionários da empresa, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente da empresa, ou informações pertencentes à empresa. Todo e qualquer usuário de recursos computadorizados da empresa tem a responsabilidade de proteger a segurança das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

1 - Exponha a empresa a danos em sua imagem ou uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados ou de informações ou ainda a perda de equipamento.

2- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

3- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - *Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessárias para a realização do negócio da empresa junto aos seus clientes.*

1. ***CONTROLE DE ACESSO AO CPD -*** *O acesso ao ambiente do CPD será controlado por equipamentos leitores de cartão e será concedido somente a pessoas autorizadas e previamente cadastradas, sendo responsabilidade da Equipe de Segurança a concessão das referidas permissões mediante solicitação do gestor do departamento de TI. Qualquer pessoa externa a empresa que porventura tenha necessidade de entrar no CPD deverá ser acompanhado por um profissional da área durante todo o tempo da visita.*

2. **DESCARTE DE INFORMAÇÕES SIGILOSAS -** *É de responsabilidade dos funcionários realizar o correto descarte de informações sigilosas utilizadas durante os processos de trabalho de modo que não seja possível a sua recuperação.*

PENALIDADES - O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar em abertura de processo administrativo para apurar as responsabilidades ou demissão.

3.4 Identificação e Classificação dos Ativos

Cada sistema de informação possui vários ativos de informação que são utilizados em conjunto para atingir o objetivo do negócio. Esses ativos de informação utilizam outros componentes críticos como software, hardware, infraestrutura de TI e estrutura física para desempenhar tarefas designadas de maneira segura e eficiente. Identificar todos esses ativos e componentes críticos e manter um registro atualizado é essencial para saber o que precisamos proteger. Uma vez que temos esse inventário, o próximo passo é classificar os ativos com base na sua criticidade em relação a confidencialidade, integridade e disponibilidade da informação. Essa classificação é necessária para implementar várias medidas de segurança.

Os ativos podem ser agrupados dentro das seguintes categorias:

- Ativos de informação: Esses são os ativos criados pela organização e são os mais difíceis de substituir. Exemplos: bancos de dados, documentação, procedimentos, planos, diagramas etc. Eles podem estar gravados em vários

tipos de mídia. Esse tipo de ativo deve ser protegido cuidadosamente durante todo seu ciclo de vida.

- Ativos de software: aplicações, sistemas, ferramentas de desenvolvimento e utilitários são parte desses ativos. Aplicações que foram desenvolvidas dentro da organização ou personalizadas são difíceis de substituir, comparados com softwares de prateleira, por isso devem ser mais bem protegidos.
- Ativos físicos: todos os dispositivos de hardware, comunicação, mídia magnética, dispositivos de infraestrutura como ar condicionado, fontes de energia. Mídias de backup, por exemplo, podem não ter um valor tão elevado por si só, mas se elas contêm informações críticas o nível de segurança deve ser aumentado.
- Serviços: serviço de comunicação e utilidades gerais como iluminação, energia, ar condicionado etc. Áreas críticas para o negócio que dependam desses serviços para funcionar os tornam críticos também.

Deve ser feita a identificação dos ativos através de um método que identifique de maneira única cada um deles. Essa identificação deve ser visível para toda a organização para evitar esforço duplicado e deve incluir: uma lista de todos os sistemas de informação incluídos no SGSI; lista de ativos e seus responsáveis; localização dos ativos;

Quadro 4 – Exemplo de classificação de ativo

Sistema de RH

Confidencialidade: Muito alta, os dados dos funcionários devem ser mantidos no nível mais alto de confidencialidade.

Integridade: Média, esses dados são verificados em várias etapas e qualquer alteração seria detectada.

Disponibilidade: Baixa, um atraso de até um dia em ter acesso a essas informações é aceitável.

Classificação dos componentes do sistema de RH:

Componente	Confidencialidade	Integridade	Disponibilidade

	Banco de Dados	Muito alta	Média	Baixa
	Servidor	Muito alta	Média	Baixa
	Fitas de backup	Muito alta	Média	Média
	Serviços	Baixa	Baixa	Baixa

3.5 Análise e Identificação dos Riscos

Após a identificação dos ativos devemos identificar as ameaças relacionadas a eles. Faça uma lista contendo todas as ameaças possíveis de acontecer, dos diversos tipos listados no item 2.2 deste trabalho. Essa lista pode ser feita com base em entrevistas, históricos ou experiência.

Faça uma análise de vulnerabilidade, vários procedimentos podem ser adotados para a realização dessa análise, como:

- Revisão de documentação: através da revisão de documentação é possível descobrir se a segurança fazia parte dos processos da empresa.
- Revisão de logs de incidente: o histórico de incidentes pode fornecer uma ótima visão sobre a vulnerabilidade dos sistemas da empresa.
- Testes de segurança: várias ferramentas de segurança podem ser usadas para identificar vulnerabilidades nos sistemas.
- Engenharia social: a engenharia social é uma das técnicas mais efetivas de ataque. Ela também pode ser usada para descobrir vulnerabilidades, que geralmente estão presentes devido à falta de conscientização ou conhecimento em segurança da informação por parte dos funcionários.
- Uso de ferramentas de análise de risco: várias ferramentas comerciais estão disponíveis para ajudar uma organização a avaliar o seu nível de segurança.

Com base nas análises feitas, cada ameaça e vulnerabilidade devem ser classificadas de acordo com sua severidade. Baixa é quando o atacante necessita de muitos recursos para explorar a vulnerabilidade. Severidade alta significa que o atacante não precisa de muitos recursos pra explorar essa vulnerabilidade e que ela tem um potencial de perda muito grande para a empresa.

O próximo passo é avaliar o nível de risco ao qual a organização está exposta. A análise de riscos pode ser feita tanto com base em estatísticas, chamada quantitativa, quanto baseada na experiência de profissionais da área, também conhecida como análise qualitativa. Ambas são ferramentas importantes no processo de identificação de riscos, porém a decisão de qual utilizar deve ser tomada com base nas características da organização.

Na abordagem quantitativa as informações sobre ataques e incidentes são coletadas com o auxílio de ferramentas computacionais específicas. O processo de análise qualitativa não requer cálculos complexos, é baseado na experiência de especialistas de segurança e tem maior agilidade, por isso geralmente as empresas tendem a adotar esse modelo.

3.6 Planejamento da Gestão de Risco

Após o diagnóstico dos riscos, o tratamento dos mesmos é escolhido com base em uma análise de custo/benefício das várias opções disponíveis, que são:

- Transferir o risco: por meio de contratos, seguros ou terceirização;
- Evitar o risco: tomar medidas suficientes para que o risco deixe de existir;
- Aceitar o risco: você está ciente de que o risco existe, porém o custo para tratá-lo é muito alto ou o risco já está em um nível considerado aceitável;
- Redução do risco: são aplicados controles de segurança a fim de reduzir esses riscos a níveis aceitáveis.

Independente da opção para tratamento de cada risco, a escolha deve ser documentada. Em um relatório final devem conter: a identificação e classificação de ativos e processos de negócio; a análise de ameaças e vulnerabilidades; a análise e classificação dos riscos; e a definição de tratamento dos riscos.

É importante também implantar uma estratégia proativa de gestão dos riscos, que consiste em um conjunto de etapas predefinidas que devem ser seguidas para impedir ataques antes que eles ocorram. Essas etapas devem avaliar quais as

vulnerabilidades do sistema e quais danos um ataque poderia causar. O resultado dessas avaliações deve ajudar a implementar normas de segurança para controlar ou minimizar os ataques e poderá também identificar padrões de ataques que serão úteis para determinar as áreas de vulnerabilidade que representam o maior risco para a empresa.

Ainda nessa etapa é elaborado o Plano de Continuidade dos Negócios, que tem objetivo de manter funcionando os serviços críticos em situações de emergência. Também são elaborados procedimentos e normas que definem detalhes a respeito da implementação da política de segurança, como responsabilidades e ações a serem tomadas para prevenir, detectar, corrigir e reportar falhas de segurança.

Como não é possível garantir total proteção contra todas as ameaças que existem, precisamos identificar os ativos mais importantes e as vulnerabilidades mais críticas, estimando o impacto que um determinado risco pode causar ao negócio, definir o tratamento que será dado a cada um e priorizar os esforços e gastos com segurança. Só então é que são implantadas as medidas de segurança.

Uma vez que a política e os requisitos de segurança tenham sidos definidos, devem ser selecionados os controles de segurança que garantam uma redução dos riscos um nível aceitável, os riscos residuais devem ser documentados e aprovados pela direção da empresa.

Devem ser considerados os controles descritos na norma ABNT NBR ISO/IEC 27002:2005 e também os descritos em outras normas de segurança, além de técnicas presentes no mercado, selecionando as que se aplicam às políticas da organização para que sejam integradas ao SGSI.

Para a seleção dos controles devem ser considerados também os seguintes critérios: relação custo/benefício; a possibilidade da utilização do mesmo controle para redução de vários riscos a níveis aceitáveis; a facilidade de gerenciamento e a possibilidade de substituição do controle.

A instituição de regras, procedimento e controles deve ser realizada tanto internamente na empresa como no acesso externo de parceiros à rede ou sistemas da empresa, de modo que nenhum acesso fique sem algum mecanismo de controle que garanta a segurança.

3.7 Implementação da Estratégia de Gestão de Risco

A implementação da estratégia de gerenciamento de risco envolve converter todo o planejamento em ações. Como um resultado das etapas anteriores você deve ter, prontos para implementação, a política de segurança, normas, procedimentos e ferramentas de segurança.

Uma vez selecionados, os controles devem ser implementados dentro do escopo estabelecido, de acordo com a estratégia de gerenciamento de riscos, e tendo em vista que esses controles não devem atrasar ou impedir a correta realização da atividade fim da empresa.

A implementação dos controles selecionados pode envolver a aquisição de tecnologia de software ou hardware, mas em alguns casos, essa implementação resulta apenas na criação de padrões e normas internas a serem obedecidas.

Alguns controles essenciais devem ser implementados na maioria das organizações, por exemplo:

- Tratamento de ameaças naturais:
    - Plano de recuperação de desastres
    - Planejamento de backup
- Tratamento de ameaças humanas:
    - Políticas de senhas
    - Controle de acesso à internet
    - Ações punitivas
- Controles técnicos
    - Controle de versão
    - Software de segurança

- Segurança de banco de dados
- Segurança de rede e telecomunicação
- Segurança de sistema operacional
- Firewall
- Gerenciamento de incidente
- Classificação de dados
- Segurança de servidores
- Proteção contra vírus
- Criptografia de dados

3.8 Elaboração da Declaração de Aplicabilidade

A norma ABNT NBR ISO/IEC 27001:2006 orienta também que é importante se elaborar uma declaração de aplicabilidade, que provê um resumo das decisões referentes ao tratamento de riscos. Essa declaração deve conter: os objetivos de controle e controles selecionados e os motivos dessa seleção; os objetivos de controle e controles já implementados; lista de objetivos de controle e controles excluídos e razões para essas exclusões.

3.9 Treinamento e conscientização dos funcionários

A gestão da segurança da informação envolve cada pessoa que interage com a informação. Todas essas pessoas tem a capacidade de causar algum dano, seja por ignorância ou más intenções. O treinamento deve explicar a todos o seu papel na garantia da segurança e suas responsabilidades sobre as informações que manipulam e garantir que cada um conheça as políticas de segurança da organização, os riscos e ameaças associadas aos ativos que lhe dizem respeito e as consequências de não realizar os procedimentos de segurança definidos.

É importante separar os programas de treinamentos por grupos específicos como: gestores, usuários finais, e departamento de TI. Criar calendários de treinamento anuais e garantir que todos os usuários foram treinados. Também se devem manter sempre os funcionários informados através de campanhas, e-mails ou pôsteres, para que os procedimentos de segurança não caiam no esquecimento.

Também é importante que sejam divulgados entre os funcionários incidentes relevantes de segurança e suas consequências para que seja aumentada a conscientização sobre a importância dos procedimentos de segurança.

Recomenda-se ainda a elaboração de um manual de segurança que contenha os documentos gerados nas várias etapas do processo, como: política de segurança; análise de risco; inventário; declaração de aplicabilidade; temos e políticas de uso dos sistemas e dos serviços oferecidos; indicadores de acompanhamento, além de incidentes registrados e classificados.

3.10 Monitoramento e Análise

Após as fases de implantação de normas de segurança e controles devemos realizar um acompanhamento constante das medidas de segurança adotadas. Para realizar essa tarefa é necessário produzir indicadores específicos que possibilitem visualizar as condições de funcionamento e desempenho do ambiente analisado, tornando possível identificar quais áreas foram bem sucedidas e quais precisam de revisões e ajustes dessas medidas.

Na fase de monitoramento são realizadas ainda as auditorias internas do SGSI, que têm a finalidade de verificar o desempenho de vários controles e medidas definidos no SGSI. Os resultados dessas auditorias devem ser documentados e todas as não conformidades devem ser corrigidas e reportadas dentro de um prazo especificado.

A eficácia das auditorias internas pode ser garantida através do uso de algumas medidas como: os auditores serem independentes; realização de planejamento e comunicação prévia; o compromisso de melhora contínua do SGSI; e alinhamento dos relatórios com as atividades referentes à segurança da informação, e com os objetivos, metas e políticas da organização.

3.11 Manutenção e Melhoria

A implementação de um SGSI não garante a melhoria repentina da segurança da informação na organização, é um processo que busca continuamente o aprimoramento do modelo de gestão da segurança da informação. Para tal, o acompanhamento e gerenciamento do fluxo com o ciclo PDCA devem ser uma constante na organização, seja através de auditorias periódicas, ou de ações de melhorias inseridas na rotina diária de administração da informação. Também é importante acompanhar, através dos relatórios de incidentes ou auditorias, as falhas de segurança reportadas e tomar as ações apropriadas que permitam uma melhoria de todo o sistema.

CONCLUSÃO

A partir desse estudo podemos concluir que garantir a segurança da informação em uma organização não é a simples implantação de medidas sem um planejamento adequado. Foi exposto que a busca histórica por solucionar problemas de segurança da informação nas empresas, levou ao desenvolvimento de padrões internacionais e normas técnicas que definem maneiras de se resguardar quanto às ameaças. Todo o processo de gestão de segurança da informação é complexo e envolve várias ações conjuntas que montam o que é chamado de Sistema de Gestão da Segurança da Informação. Vimos também que a implantação e a operação desse sistema necessitam de uma análise profunda do ambiente computacional e organizacional da empresa. Além disso, a existência de um SGSI em operação na empresa aumenta o nível de profissionalismo da organização e traz mais confiabilidade aos clientes.

Este trabalho contribuiu para a definição de um método para implantação de um SGSI, conforme orientações da norma ABNT NBR ISO/IEC 27001:2006. Trouxe também conceitos de segurança da informação que subsidiam o entendimento, implantação e operação do SGSI. Todo o método apresentado foi escrito para que seja de fácil entendimento e aplicação, e aderente ao ciclo PDCA, tornando-o de fácil implementação e podendo ser integrado com tranquilidade ao processo de gestão da empresa.

REFERÊNCIAS

ALVES, Gustavo Alberto. **Segurança da Informação – Uma Visão Inovadora da Gestão**. RJ: Ed. Ciência Moderna, 2006.

Associação Brasileira de Normas Técnicas - ABNT. **Norma ABNT NBR ISO/IEC 27005:2008**.

Associação Brasileira de Normas Técnicas - ABNT. **Norma ABNT NBR ISO/IEC 27001:2006.**

Associação Brasileira de Normas Técnicas – ABNT. **Norma ABNT NBR ISO/IEC 27002:2005**.

BEAL, Adriana. **Segurança da Informação – Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. SP: Ed. Atlas, 2008.

CHESWICK, W., BELLOVIN, S. M., RUBIN. A. D. **Firewalls e Segurança na Internet**. 2. Ed. Rio Grande do Sul: Bokman, 2005.

DAWEL, George. **A Segurança da Informação nas Empresas**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2005.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000.

FITZGERALD, Jerry; DENNIS, Alan. **Comunicação de Dados Empresariais e Redes**, Rio de Janeiro: LTC, 2005.

HATCH, Brian; LEE, James; KURTZ, George. **Segurança contra Hackers**. São Paulo: Futura, 2003.

KUROSE, J. F., ROSS, K. W. **Redes de Computadores e a Internet**. São Paulo. Addison Wesley, 2003.

MICHAELIS. **Moderno Dicionário da Língua Portuguesa**. Disponível em: http://michaelis.uol.com.br/. Acesso em: 28 de maio de 2013.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de Redes:** em ambientes cooperativos. 2. ed. São Paulo: Futura, 2003.

PFLEEGER, Charles P. **Security in Computing**. 2. Ed. New Jersey, USA: Prentice Hall, 1997.

ROESCH, Martin. **Snort Users Manual – The Snort Project**. Sourcefire Inc, 2006.

SÊMOLA, M. **Gestão da Segurança da Informação:** Uma visão executiva. Rio de Janeiro: Campus, 2003.

STALLINGS, William. **Criptografia e segurança de redes**. 4. Ed. São Paulo: Pearson Prentice Hall, 2008.

TANENBAUM, Andrew S. **Redes de Computadores**. Tradução Daniel Vieira. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

The Internet Engineering Task Force – IETF. **RFC 2828**. Disponível em: http://www.ietf.org/rfc/rfc2828.txt . Acesso em 05 de junho de 2013.

WADLOW, Thomas. **Segurança de Redes - Projeto e Gerenciamento de Redes Seguras**. São Paulo: Campus, 2000.