Claretiano
CENTRO UNIVERSITÁRIO

SEGURANÇA
E AUDITORIA DE SISTEMAS

CURSOS DE GRADUAÇÃO – EAD

Segurança e Auditoria de Sistemas – *Prof. Alex Sandro Scarpim*

Olá! Meu nome é **Alex Sandro Scarpim**. Sou graduado em Engenharia Elétrica com ênfase em Telecomunicações pela Pontifícia Universidade Católica de Campinas (PUCCAMP) e curso, atualmente, a Especialização em Gestão de Projetos em TI na Veris Faculdades. Profissionalmente, atuo como analista de suporte à rede e sou tutor presencial do Centro Universitário Claretiano no polo de Campinas-SP. Espero que possamos realizar um ótimo trabalho juntos. Tenha sucesso!

E-mail: ascarpim@gmail.com

Alex Sandro Scarpim

SEGURANÇA E AUDITORIA DE SISTEMAS

Batatais
Claretiano
2013

Versão: dez./2013

658.472 S311s

Scarpim, Alex Sandro
Segurança e auditoria de sistemas / Alex Sandro Scarpim – Batatais, SP : Claretiano, 2013.
158 p.

ISBN: 978-85-8377-115-9

1. Análise de Riscos. 2. Ameaças a um sistema computacional. 3. Controles de acesso lógico. 4. Auditoria e governança de TI. I. Segurança e auditoria de sistemas.

CDD 658.472

Corpo Técnico Editorial do Material Didático Mediacional
Coordenador de Material Didático Mediacional: J. Alves

Preparação
Aline de Fátima Guedes
Camila Maria Nardi Matos
Carolina de Andrade Baviera
Cátia Aparecida Ribeiro
Dandara Louise Vieira Matavelli
Elaine Aparecida de Lima Moraes
Josiane Marchiori Martins
Lidiane Maria Magalini
Luciana A. Mani Adami
Luciana dos Santos Sançana de Melo
Luis Henrique de Souza
Patrícia Alves Veronez Montera
Rosemeire Cristina Astolphi Buzzelli
Simone Rodrigues de Oliveira

Bibliotecária
Ana Carolina Guimarães – CRB7: 64/11

Revisão
Cecília Beatriz Alves Teixeira
Felipe Aleixo
Filipi Andrade de Deus Silveira
Paulo Roberto F. M. Sposati Ortiz
Rodrigo Ferreira Daverni
Sônia Galindo Melo
Talita Cristina Bartolomeu
Vanessa Vergani Machado

Projeto gráfico, diagramação e capa
Eduardo de Oliveira Azevedo
Joice Cristina Micai
Lúcia Maria de Sousa Ferrão
Luis Antônio Guimarães Toloi
Raphael Fantacini de Oliveira
Tamires Botta Murakami de Souza
Wagner Segato dos Santos

Claretiano - Centro Universitário
Rua Dom Bosco, 466 - Bairro: Castelo – Batatais SP – CEP 14.300-000
cead@claretiano.edu.br
Fone: (16) 3660-1777 – Fax: (16) 3660-1780 – 0800 941 0006
www.claretianobt.com.br

Fazemos parte do ***Claretiano - Rede de Educação***

SUMÁRIO

CADERNO DE REFERÊNCIA DE CONTEÚDO

UNIDADE 1 – INTRODUÇÃO À SEGURANÇA E À AUDITORIA DE SISTEMAS

UNIDADE 2 – AMEAÇAS A UM SISTEMA COMPUTACIONAL

UNIDADE 3 – CONTROLES DE ACESSO LÓGICO

EAD

Caderno de Referência de Conteúdo

CRC

Conteúdo

Introdução à Segurança de Informações. Política de Segurança de Informações. Análise de Riscos. Ameaças a um sistema computacional (*Spoofing*, *DOS*, *Smurf*, Engenharia Social, *Syn Flood*). Controles de acesso lógico (criptografia, assinatura digital, *firewall*). Auditoria da Tecnologia da Informação. Metodologia para Auditoria de Informática.

1. INTRODUÇÃO

Seja bem-vindo!

Segurança e Auditoria de Sistemas é um dos *Cadernos de Referência de Conteúdos* que compõem os Cursos de Graduação do Centro Universitário Claretiano na modalidade EaD. Neste material, você encontrará o conteúdo dividido em cinco unidades.

O *Caderno de Referência de Conteúdo* de *Segurança e Auditoria de Sistemas* abordará os principais conceitos de segurança de um sistema de informação, destacando o papel da informação

como elemento importante para a geração de conhecimento, a tomada de decisões e, principalmente, o valor que agregará ao negócio.

A princípio, os sistemas trabalhavam isoladamente, e os riscos de ataques estavam sujeitos a atividades internas das corporações, facilitando, assim, sua identificação e resolução. Nos dias atuais, as informações sofrem mais ataques, os quais poderão partir de qualquer parte do mundo.

Para isso, basta que o dispositivo (computador, celular, entre outros) esteja conectado à internet. Com o intuito de evitar ou diminuir os impactos causados por ataques aos sistemas de informação, é realizado o estudo dos riscos, denominado "análise de risco", e seus resultados serão utilizados para a elaboração de uma política de segurança aplicável à organização ou à instituição.

As políticas de segurança ajudam a garantir um cenário menos propício aos ataques, utilizando-se de mecanismos de controle de acesso lógico às informações. Os mecanismos mais comuns são criptografia de dados, assinaturas digitais, certificados digitais e implementação de um serviço de *firewall*.

Uma vez definidas as regras da política de segurança, esta deverá obter o pleno apoio da direção da empresa para garantir sua credibilidade e cumprimento pelos demais usuários dos sistemas. Também deverá ser divulgada amplamente aos colaboradores, para que todos saibam dos seus direitos, deveres e punições aplicáveis caso a política seja desrespeitada.

Como em todas as outras áreas, os processos envolvidos em um sistema de informação devem ser constantemente revisados e atualizados, ou seja, melhorias frequentemente devem ser implementadas, buscando resultados satisfatórios e eficientes.

Para tal, os processos da Tecnologia da Informação (TI) deverão ser auditados, isto é, controlados por meio do uso de metodologias apropriadas, tendo como resultado relatórios de aponta-

mentos de conformidades. O objetivo da auditoria é descobrir as irregularidades presentes em departamentos e centros de processamento das organizações, bem como identificar os pontos que irão desagradar à direção, tendo como finalidade sua correção.

Após esta introdução, apresentaremos, no Tópico 2, algumas orientações de caráter motivacional, dicas e estratégias de aprendizagem que poderão facilitar o seu estudo.

Desejamos a você bons estudos!

2. ORIENTAÇÕES PARA ESTUDO

Abordagem Geral

Neste tópico, apresenta-se uma visão geral do que será estudado neste *Caderno de Referência de Conteúdo*. Aqui, você entrará em contato com os assuntos principais deste conteúdo de forma breve e geral e terá a oportunidade de aprofundar essas questões no estudo de cada unidade. Desse modo, esta Abordagem Geral visa fornecer-lhe o conhecimento básico necessário a partir do qual você possa construir um referencial teórico com base sólida – científica e cultural – para que, no futuro exercício de sua profissão, você a exerça com competência cognitiva, ética e responsabilidade social.

Estudaremos sobre segurança e auditoria de sistemas, um conceito bastante abrangente e de extrema importância na área da TI, que tem como objetivos:

1) Caracterizar problemas de segurança e avaliar o risco e seu impacto. Você deverá assimilar os aspectos teóricos sobre os problemas ou riscos relacionados à segurança da informação, bem como os impactos resultantes desses incidentes de segurança.

2) Descrever políticas de segurança e técnicas utilizadas para aumento da segurança. Você conhecerá as características de uma política de segurança e também deverá desenvolver uma política com o objetivo de colocar em prática os conhecimentos teóricos.
3) Conhecer as principais técnicas utilizadas para comprometer um sistema. Você conhecerá alguns exemplos de ferramentas utilizadas para quebra de segurança dos sistemas de informação e, consequentemente, seu comprometimento.
4) Conhecer e aplicar formas de inibir as principais ameaças a um sistema informatizado. Serão apresentadas as técnicas e as ferramentas utilizadas pelos administradores de rede para inibição das ameaças aos sistemas computacionais.
5) Usar criptografia, assinatura e certificados digitais. Você entrará em contato com os mecanismos utilizados para garantir a segurança da informação, ou seja, conhecerá o funcionamento das técnicas de criptografia, assinatura e certificados digitais.
6) Definir estratégias de segurança em uma rede por meio do conceito de *firewall*. Você deverá entender o funcionamento e a aplicabilidade do conceito de *firewall* em uma rede de dados.
7) Definir uma equipe de auditoria e uma área a ser auditada, estabelecendo metodologias e procedimentos a serem adotados. Você estudará os conceitos teóricos sobre auditoria e desenvolverá a percepção do papel importante do auditor nesse processo. Além disso, entenderá os objetivos de uma auditoria na área de TI.
8) Discutir sobre o planejamento da execução de uma auditoria. Você poderá discutir sobre as fases de planejamento e execução de uma auditoria com base nos conceitos teóricos apresentados.
9) Elaborar um relatório final de auditoria. Você fará um relatório final de auditoria, aplicando os conhecimentos teóricos, bem como entendendo os objetivos de um relatório escrito e as áreas a que se destina.

De uma maneira geral, o *Caderno de Referência de Conteúdo* de *Segurança e Auditoria de Sistemas* trata dos conceitos teóricos e práticos da segurança de um sistema computacional.

Desse modo, na Unidade 1, você estudará as características de segurança da informação, como confiabilidade, disponibilidade e integridade de dados. Além disso, será apresentada a importância da elaboração e da implementação de uma política de segurança na organização e suas propriedades ou características.

Primeiramente, precisamos entender os fatores que contribuem ao cenário de dependência em que as organizações hoje se encontram em relação às informações. Isso se dá porque as informações são consideradas o seu bem mais valioso. Como a forma de registrar as informações se tornou digital, ou seja, são armazenadas em ambientes informatizados, também surge a necessidade de implementar uma política que mantenha a informação íntegra, disponível e acessível, para que ela seja acessada somente por quem é de direito.

O controle de acesso lógico tem por base a utilização de senhas. O termo **acesso lógico** pode ser entendido como o acesso ao ambiente (sistemas computacionais) ou acesso ao conteúdo informacional frequentemente associado à área da informática.

Os níveis de acesso às informações variam de organização para organização, e, em alguns casos, na ausência de uma política de segurança, o cuidado com os acessos nem é levado em consideração, caracterizando, assim, um ambiente passivo de ocorrências de incidentes de segurança. Apresentaremos a seguir os três princípios básicos de um sistema de segurança da informação.

1) **Confidencialidade dos dados**: somente pessoas com as devidas permissões devem ter acesso aos dados, ou seja, deve-se manter a confidencialidade dos dados.
2) **Integridade dos dados**: diz respeito à proteção contra alteração dos dados, isto é, deve-se manter a integridade dos dados.

3) **Disponibilidade de dados**: trata-se do ininterrupto acesso aos dados ou serviços.

No processo de gerenciamento da segurança da informação, deve-se trabalhar, inicialmente, na identificação e análise dos riscos de incidentes de segurança, coletando informações sobre o seu grau de existência em determinado ambiente da organização, e, por fim, elaborar um plano de segurança. Tomemos como exemplo o fator de risco *hardware*.

A próxima etapa é listar as ameaças que envolvem os ativos de informações relacionadas a esse fator. Nesse exemplo, foram identificadas ameaças que vão desde oscilações de energia elétrica, falhas de climatização, instalações inadequadas, até danos físicos. Depois de identificadas, as ameaças devem ser tratadas pontualmente, sempre levando em consideração a relação custo/benefício da implementação da segurança.

Depois de identificadas e listadas as ameaças passíveis de tratamento, uma política de segurança deve ser elaborada. Essa política abrange um conjunto de controles que, uma vez implementados, buscam diminuir as vulnerabilidades do sistema de informação. Uma vez colocada em prática dentro da organização, tal política deve minimizar a probabilidade de ocorrência, diminuir os prejuízos causados por eventuais acontecimentos e elaborar procedimentos para recuperação de desastres.

Apesar do papel fundamental no processo de manutenção da segurança da informação, a política de segurança ainda é pouco difundida. Porém, antes da aplicação da política, é essencial o estabelecimento de uma política educacional em relação à segurança, divulgando-a por meio de palestras, *e-mail* informativo, apresentações, enfim, pelos meios de divulgação disponíveis na organização.

Na Unidade 2, serão apresentadas as principais ameaças a um sistema computacional, ou seja, as técnicas utilizadas para acesso a dados ou informação confidencial por pessoas não auto-

rizadas. Serão abordados exemplos de ataques como o de engenharia social, no qual o invasor normalmente se passa por outra pessoa para conseguir acesso aos sistemas de modo geral. Também serão discutidos as vulnerabilidades e os possíveis tipos de ataque às redes Wi-Fi, bem como os mecanismos empregados para a segurança da informação.

A partir da identificação das vulnerabilidades de um sistema, podemos adotar medidas para contornar ou até mesmo anular tais ameaças. Classificados de acordo com o objetivo a ser alcançado, os tipos de ataques são: acesso não autorizado, impedimento de uso do equipamento e roubo de informações. Seja qual for o tipo, os ataques são bem-sucedidos por causa de falta de segurança ou vulnerabilidades não cobertas pela política de segurança da organização.

Dentre os vários tipos de ameaças apresentados neste *Caderno de Referência de Conteúdo*, uma das formas mais comuns de ataque é denominada **DoS** (*Denial of Service*), que tem por prática buscar a interrupção de serviços e/ou recursos da vítima enviando uma grande quantidade de requisições simultâneas a um servidor. De maneira resumida, o DoS é causado pela grande quantidade de requisições enviadas ao servidor. Dessa maneira, recursos finitos, como memória e capacidade de processamento, são totalmente consumidos, e os serviços que deveriam ser providos aos clientes legítimos deixam de ser respondidos.

Os ataques de negação de serviço apresentam-se de duas formas distintas.

Na primeira, denominada **ataque direto**, o atacante envia requisições diretamente ao servidor. Nesse caso, as consequências são limitadas, pois somente uma estação atuando no ataque dificilmente conseguirá consumir todo o recurso disponível de um servidor.

Já na segunda forma, denominada **DDoS** (*Distributed Denial of Service*), o ataque é realizado por várias estações simultanea-

mente, ou seja, inúmeras requisições são enviadas ao servidor da vítima, garantindo que os seus recursos se tornem indisponíveis. Para tal, faz-se necessário um alto nível de planejamento por parte do atacante, pois deve assumir o controle de várias estações, infectando-as com programas similares a vírus que se propagam automaticamente.

As estações infectadas – conhecidas como *daemon*, ou zumbi – aguardam um comando do atacante para que iniciem as requisições ao servidor, causando sobrecargas sobre o *link* e, principalmente, sobre a memória.

Uma forma alternativa e aprimorada de ataque que busca driblar as técnicas de proteção atuais é conhecida como **engenharia social**, a qual recebe esse nome por ter como objetivo a captura de informações das vítimas sem o uso de força bruta, ou seja, o atacante utiliza-se de armadilhas para induzir os usuários a fornecerem deliberadamente informações que, em um primeiro momento, não parecem ser importantes, mas, quando reunidas, pode-se observar o quão eficiente é essa forma de ataque.

Os atacantes fazem uso de ferramentas de comunicação disponíveis na internet, como *e-mails*, *sites*, mensagens instantâneas e comunidades de relacionamento, para realizarem os ataques às vítimas.

Além das ameaças já citadas, a popularização das redes Wi-Fi oferece novas maneiras de explorar a vulnerabilidade em um sistema computacional, pois, diferentemente da rede cabeada, as redes Wi-Fi muitas vezes não se restringem aos limites físicos da organização. Pontos de acesso público, por exemplo, onde as redes Wi-Fi estão publicadas e disponíveis para uso, tornaram-se os principais alvos de ataques.

Protocolos foram desenvolvidos para garantir a segurança na comunicação das redes Wi-Fi, como o WEP (*Wired Equivalent Privacy*) e seu sucessor, denominado WPA (Wi-Fi *Protected Access*). Ambos utilizam técnicas de criptografia antes da transmissão propriamente dita.

Na Unidade 3, você conhecerá os controles de acesso lógico e sua correta aplicação, dependendo do tipo de ameaça a ser tratada. O uso de técnicas de criptografia procura garantir a segurança da informação por meio da cifragem, ou codificação, dos dados. Para prevenir acessos indesejados à rede e, consequentemente, às informações, é empregado o uso do *firewall*, que trabalha com a aplicação de regras predefinidas pelo administrador da rede.

Conforme já mencionado, a criptografia, ou cifragem, caracteriza-se por esconder as informações, tornando-as seguras, uma vez que, para sua compreensão, é necessária a decifragem dos dados. Destacamos, nesse cenário, a criptografia simétrica, a qual codifica a informação se utilizando de algoritmos que compartilham a mesma chave, e a criptografia de chave pública, que, por sua vez, trabalha com duas chaves distintas, a privada e a chave pública.

Outro mecanismo utilizado para garantir a segurança e a autenticidade da informação é a assinatura digital. Essa é uma maneira digital de autenticação da informação, ou seja, podemos identificar o emissor da mensagem por meio da sua assinatura digital. Para isso, ela deve possuir autenticidade, integridade e irretratabilidade.

A comprovação de uma assinatura digital é realizada por meio do cálculo ou comparação entre o resumo criptográfico do documento, com a decifragem da assinatura, e a chave pública. Se a comparação identificar que ambos são iguais, a assinatura está correta e o documento está íntegro. Em contrapartida, se forem diferentes, a assinatura está incorreta ou o documento pode ter sido alterado.

A criptografia atualmente, em especial a criptografia assimétrica, é baseada na complexidade de solucionar alguns passos matemáticos. A complexidade em solucionar esses passos é não polinomial, ou seja, mesmo utilizando uma chave de tamanho não muito grande, o tempo para solução chega a ultrapassar os 100 anos, o que torna a tarefa humanamente quase impossível. Po-

rém, com o surgimento da computação quântica, esses problemas podem ser resolvidos em uma fração de tempo muito menor, pois a computação quântica vale-se de vários testes simultâneos, ou seja, eles podem ser realizados ao mesmo tempo.

Essa inovação tecnológica colocaria em risco todas as formas e técnicas criptográficas utilizadas atualmente para quem possui um computador quântico, o que torna necessário o desenvolvimento de novas técnicas de criptografia baseadas em algoritmos quânticos. Em razão desse avanço, muitos países colocaram a criptografia como problema de segurança nacional e estão investindo, cada vez mais, na procura de uma nova forma de criptografar suas informações confidenciais.

O Algoritmo de Shor é muito conhecido e se vale da computação quântica, ou seja, uma vez implementado em um computador quântico, é capaz de fatorar grandes números inteiros com tempo de resposta muito baixo. As chaves públicas RSA (Rivest, Shamir e Adelman) podem ser quebradas com a utilização desse algoritmo.

Finalmente, o certificado digital é um mecanismo eletrônico utilizado para garantir a associação de uma pessoa a uma chave pública e, normalmente, contém as informações básicas descritas a seguir:

1) Nome da pessoa ou entidade a ser associada à chave pública.
2) Período de validade do certificado.
3) Chave pública.
4) Nome e assinatura da entidade que assinou o certificado.
5) Número de série.

De acordo com o Instituto Nacional de Tecnologia da Informação − ITI (2011):

> Um exemplo comum do uso de certificados digitais é o serviço bancário provido via Internet. Os bancos possuem certificado para autenticar-se perante o cliente, assegurando que o acesso está real-

mente ocorrendo com o servidor do banco. E o cliente, ao solicitar um serviço, como por exemplo, acesso ao saldo da conta corrente, pode utilizar o seu certificado para autenticar-se perante o banco.

Serviços governamentais também têm sido implantados para suportar transações eletrônicas utilizando certificação digital, visando proporcionar aos cidadãos benefícios como agilidade nas transações, redução da burocracia, redução de custos, satisfação do usuário, entre outros. Alguns destes casos de uso são:

GOVERNO FEDERAL: o Presidente da República e Ministros têm utilizado certificados digitais na tramitação eletrônica de documentos oficiais, que serão publicados no Diário Oficial da União. Um sistema faz o controle do fluxo dos documentos de forma automática, desde a origem dos mesmos até sua publicação e arquivamento.

ESTADO DE PERNAMBUCO: primeiro estado brasileiro a utilizar a Certificação Digital. A Secretaria de Fazenda de Pernambuco disponibilizou um conjunto de serviços pela Internet com base na certificação digital que proporcionou diversos benefícios como: entrega de diversos documentos em uma única remessa; redução drástica no volume de erros de cálculo involuntários; apuração automática dos impostos; minimização de substituições de documentos e redução de custos de escrituração e armazenamento de livros fiscais obrigatórios.

IMPRENSA OFICIAL DO ESTADO DE SÃO PAULO: implantou certificação digital de ponta a ponta em seu sistema que automatiza o ciclo de publicações na Internet, permitindo a eliminação das ligações interurbanas e dos constantes congestionamentos telefônicos em horários de pico, uma vez que se utiliza a Internet com garantias de sigilo e privacidade, além da obtenção de garantia de autoria por parte do autor das matérias.

Apesar das facilidades oferecidas pela certificação digital, faz-se necessário um alerta: o seu uso não torna as transações realizadas isentas de responsabilidades. Caso não haja proteção adequada para essas transações, como antivírus, elas podem estar vulneráveis a ataques virtuais.

O *firewall* tem a finalidade de prevenir acessos indesejados às redes de computadores, que pode ser implementado por meio de *software* ou aplicativo executado por um computador comum, como também por intermédio da instalação de um *hardware* específico interligado à rede de comunicação de dados.

Sua aplicação ocorre em redes privadas que possuem conexão com a rede externa, isto é, os computadores locais necessitam acessar aplicações e/ou ferramentas externas e, para isso, utilizam-se da internet. Assim, todo o tráfego de entrada e saída da rede passa pelo *firewall*, que realiza uma verificação e bloqueia o acesso, obedecendo aos critérios de segurança especificados pelo administrador da rede.

Para realização de sua função, existem algumas técnicas de implementação do *firewall*. Uma delas é conhecida como "filtros de pacotes", pois, nessa técnica, os pacotes são filtrados de acordo com as linhas de comando configuradas no roteador, permitindo ou bloqueando o tráfego. Tal controle se baseia nos endereços IP de origem e destino dos pacotes, bem como nas portas de comunicação TCP e UDP, permitindo, assim, aos administradores conceder ou negar o acesso aos serviços, por exemplo, em ambos os sentidos da transmissão.

Outra técnica bastante conhecida são os *gateways* de aplicação. Normalmente, um *firewall* é considerado um *gateway* de segurança que controla o acesso a uma rede. O *gateway* de aplicação atua na camada de aplicação e tem como função a aplicação de mecanismos de segurança em aplicações específicas, como servidores FTP (*File Transfer Protocol*) e Telnet. Também oferece melhor proteção do que filtros de pacotes, porém essa técnica pode provocar uma diminuição de *performance* da rede.

Por fim, a técnica denominada "servidores *proxy*" trata da configuração de um cliente (navegador web) e um servidor real, no qual o aplicativo ou *software* (*proxy*) é instalado. O *proxy* verifica todos os pedidos feitos ao servidor e verifica se ele mesmo pode executar esses pedidos. Em caso negativo, ele transmite o pedido para o servidor real.

Uma das vantagens de utilização do *proxy* é a melhoria de desempenho, pois os pedidos feitos pelo usuário ao servidor ficam armazenados por um determinado intervalo de tempo. Assim,

caso ocorra uma nova requisição que já se encontre armazenada nos registros do servidor de *proxy*, o tempo de resposta para o acesso é bem menor.

Na Unidade 4, você terá a oportunidade de aprender o conceito de auditoria voltado à TI. Além disso, você terá contato com as metodologias utilizadas para auditoria de informática e com os requisitos de conformidade. As conformidades e as não conformidades são apontadas por meio de relatórios para posteriores atualizações e/ou correções nos processos auditados, lembrando que a atuação humana nesse processo é importante, isto é, a função do auditor é que define o sucesso de uma auditoria.

Iniciemos por uma definição de auditoria: atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais com o objetivo de verificar sua conformidade com certas políticas institucionais, normas e padrões. Seu objetivo principal é realizar apontamentos de irregularidades em departamentos e nos centros de processamento das empresas, identificar os pontos que irão desagradar à alta administração para que estes possam ser corrigidos, bem como propor melhorias na execução dos processos.

A auditoria normalmente deverá abranger áreas estratégicas da TI, conforme apresentado a seguir:

1) Recuperação de desastre.
2) Capacidade dos sistemas.
3) Desempenho dos sistemas.
4) Desenvolvimento de sistemas.
5) Sistemas financeiros.
6) Rede de telecomunicações.
7) Segurança de informação.

Uma das peças mais importantes e fundamentais no processo de auditoria é o auditor. Ele é considerado uma das partes mais importantes do processo de auditoria, pois, além de ser um profissional capacitado, deve ter grande conhecimento na área da TI e de todas as suas fases apresentadas anteriormente.

A auditoria de sistemas é responsável pela revisão e avaliação dos controles do sistema de informação. Tem como objetivo manter a autenticidade e a integridade dos dados, além de proteger os ativos da organização. Geralmente, as empresas voltam sua atenção para a proteção dos ativos físicos e financeiros, deixando de lado os seus ativos de informação, porém, da mesma maneira que os ativos tangíveis, as informações relacionam-se com os fatores de produção tradicionais: capital, mão de obra e processos.

Dessa maneira, do ponto de vista do negócio, as informações são consideradas um ativo da empresa. A atividade de auditoria pode ser dividida em três fases: planejamento, execução e relatório. Os tipos mais comuns são classificados quanto ao órgão fiscalizador, à forma de abordagem do tema e ao tipo ou área envolvida.

Os tipos relacionados ao órgão fiscalizador são: auditoria interna, auditoria externa e auditoria articulada.

A auditoria de sistemas é responsável pela análise da gestão de recursos, focando especialmente os aspectos de eficiência, eficácia, economia e efetividade. Ela abrange o ambiente de TI de forma global e analisa aspectos como segurança física (acesso físico ao ambiente dos servidores) e segurança lógica (os sistemas computacionais), planejamento de contingências e operação do CPD (Centro de Processamento de Dados). Pode estender-se à organização do departamento de TI, analisando aspectos administrativos da organização, como políticas, padrões e procedimentos, responsabilidades organizacionais, gerência de pessoal e planejamento de capacidade.

Ainda dentro da fase de planejamento, uma vez definida a equipe, a próxima fase será a escolha da metodologia a ser adotada. Uma das metodologias mais frequentemente utilizadas adota a prática de entrevistas, que são realizadas com os funcionários da organização, apresentando o plano da auditoria que será realizado, coletando dados e identificando falhas e irregularidades. As entrevistas podem ser:

1) **Entrevista de apresentação**: a ser realizada com gerentes, funcionários e diretores para apresentação do plano de auditoria e cronograma de atividades.
2) **Entrevista de coleta de dados**: coleta dados sobre o sistema e os ambientes de informática.
3) **Entrevista de discussão das deficiências encontradas**: são discutidos abertamente os pontos críticos, e as justificativas são apresentadas para tais apontamentos.
4) **Entrevista de encerramento**: reunião com os dirigentes da entidade auditada para agradecimentos e apresentação dos resultados, recomendações, comentários e entrega dos relatórios da auditoria.

Durante o processo de auditoria, a equipe deve reunir evidências confiáveis, relevantes e úteis, para que os objetivos da auditoria sejam alcançados. As evidências apresentam-se divididas em quatro grupos: evidências físicas, evidências documentárias, evidências fornecidas pelo auditado e evidências analíticas.

O relatório escrito de uma auditoria tem como objetivo apresentar evidências e conclusões, devendo ser claro e objetivo. Esse documento pode ser encaminhado à diretoria da organização quando for solicitado, a fim de identificar falhas em sua própria administração; ao organismo que financia a entidade auditada, como forma de proteger seus investimentos; ou ao organismo responsável pelo controle de auditoria.

Por fim, os planos de contingência e de recuperação de desastres também devem ser submetidos a auditorias. Esses planos – também conhecidos como "planos de continuidade" – apresentam medidas operacionais estabelecidas e documentadas para serem seguidas no caso de ocorrer alguma indisponibilidade dos recursos de informática, evitando-se que o tempo no qual os equipamentos ficaram parados acarrete perdas materiais aos negócios da empresa.

Tais planos são de responsabilidade da diretoria da área de TI (ambientes complexos), do gerente de TI (ambientes moderados) e do encarregado ou dos analistas de sistemas responsáveis pela administração da rede (ambiente simples). No entanto, para que as medidas de contingência sejam efetivas, a alta direção precisa apoiá-las, uma vez que envolvem objetivos estratégicos da organização. O objetivo da auditoria do plano de contingência e recuperação de desastres é assegurar que:

1) Os planos atendam todas as necessidades de contingências.
2) Os planos sejam suficientemente abrangentes nos aspectos físicos e lógicos, de rede, de propriedades intelectuais, de pessoas etc.
3) A equipe de contingência esteja preparada para as eventualidades.
4) Os planos sejam testados frequentemente.
5) Os *backups* sejam atualizados.
6) As técnicas de recuperação dos *backups* sejam transparentes e de baixa complexidade.
7) Os relatórios gerenciais sirvam para facilitar o acompanhamento dos procedimentos.
8) Os relatórios apresentem informações confiáveis.

Como podemos notar, a informação é um dos bens mais valiosos para as pessoas e organizações nos dias de hoje, e garantir sua segurança e integridade é de fundamental importância, seja no âmbito particular, seja no corporativo, no qual as informações podem definir os rumos no mundo dos negócios.

Você poderá encontrar várias referências sobre esse assunto nas *E-Referências* e nas *Referências Bibliográficas* deste CRC.

Na Unidade 5, você terá a oportunidade de entrar em contato com os principais conceitos de Governança da Tecnologia da Informação, que a cada dia ganha mais destaque como prática dentro das organizações. Além disso, serão apresentados os principais modelos de melhores práticas utilizados atualmente pelo mercado profissional: o modelo COBIT (*Control Objectives for Information*

and Related Technology) e o modelo ITIL (*Information Technology Infrastructure Library*).

Iniciaremos pela definição dos conceitos de Governança da TI. De acordo com o IT Governance Institute (2005):

> A governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização.

Diante da definição apresentada, conclui-se que, para obtenção do sucesso do programa de Governança da TI, são necessários o engajamento e o comprometimento dos membros da alta direção da organização.

A disposição da governança contempla o chamado "Ciclo da Governança de TI", que é constituído das seguintes etapas: alinhamento estratégico; decisão, compromisso, priorização e alocação de recursos; estrutura, processos, operações e gestão; e medição do desempenho.

A descrição de cada uma das etapas será feita no conteúdo da Unidade 5, que, como vimos, também trará a apresentação dos modelos de melhores práticas COBIT e ITIL. Vamos iniciar pelo modelo COBIT.

O COBIT pode ser definido como um conjunto de diretrizes ou melhores práticas dirigido à Governança da TI. Foi inicialmente idealizado para servir como uma ferramenta de controle para processos da área de TI. Após várias atualizações e aperfeiçoamentos, hoje se encontra disponível na Versão 5, de 2011, que tem como foco o atendimento às necessidades atuais e futuras das partes interessadas que se alinham com o pensamento atual de governança corporativa e práticas de gestão em TI.

O modelo do COBIT representa todos os processos encontrados nas funções da TI, tanto para a operação quanto para os gerentes de negócios, uma vez que possibilita a criação de uma via comum entre as necessidades de execução (equipe operacional) e a visão que os executivos desejam ter para governar. A base de

sustentabilidade da Governança da TI, segundo o COBIT, pode ser representada por cinco áreas. São elas: alinhamento estratégico; agregação de valor; gerenciamento de riscos; gerenciamento de recursos; e medição de desempenho.

São responsabilidades do COBIT a integração e a institucionalização de boas práticas de planejamento e organização, aquisição e implementação, entrega e suporte, monitoramento e avaliação de desempenho de TI. Uma vez implantada integralmente, a Governança da TI permite a prática eficiente de gestão sobre os investimentos em tecnologia pelas organizações, transformando-a em aumento de benefícios, oportunidades de negócio e vantagem competitiva no mercado.

O COBIT utiliza-se de uma estrutura (*framework*) cuja ideia principal é a de atender às necessidades do controle organizacional relacionadas à Governança de TI, na qual as características principais são o foco nos requisitos de negócio, a orientação para uma abordagem de processos, a utilização de mecanismos de controle e o direcionamento para análise das medições e indicadores de desempenho obtidos durante o período (FERNANDES, 2008).

Uma vez seguido o modelo de referência fornecido pelo COBIT, qualquer usuário de uma determinada organização deve ser capaz de distinguir e gerenciar atividades de TI, por meio da utilização do ciclo tradicional de melhoria contínua apresentado a seguir:

1) Planejar.
2) Construir.
3) Executar.
4) Monitorar.

O COBIT identificou quatro domínios que retratam os agrupamentos existentes em uma determinada organização padrão de TI. Cada domínio abrange 34 processos, que buscam garantir a completa gestão de TI.

Um dos desafios enfrentados por muitas organizações diz respeito à definição da visualização do nível de profundidade a ser adotado pelos mecanismos de controle e medições de desempenho. Essas medidas devem ser realizadas com foco no cenário atual, identificando aspectos que precisam de melhoria, como também providenciando o monitoramento dessas ações de forma sistemática, atentando-se sempre para a relação custo/benefício do controle.

O COBIT trata a maturidade do gerenciamento e o controle dos processos de TI por meio de um método de pontuação do seu nível de maturidade: (0) não existente a (5) otimizado.

A implementação do COBIT independe do tamanho e grau de maturidade das organizações.

A seguir, trataremos do modelo de boas práticas do ITIL.

Os processos na área de TI apontavam para uma necessidade de padronização, como também de melhoria dos níveis de qualidade dos serviços prestados, resultando, assim, na criação do modelo ITIL. Depois de algumas revisões, em 2007, foi lançada a Versão 3 da ITIL, que apresenta a organização dos processos de gerenciamento de serviços por intermédio de uma estrutura do ciclo de vida de serviço. Nessa última versão, sobressai o conceito de integração da TI ao negócio e a possibilidade de convergência com os demais padrões de gestão e governança, como, por exemplo, COBIT, PMBOK (*Project Management Body of Knowledge*), CMMI (*Capability Maturity Model Integration*) etc.

A ITIL pode ser definida como um conjunto de publicações ou uma biblioteca que contém as melhores práticas utilizadas na gestão dos serviços de TI, as quais foram desenvolvidas a partir do trabalho e da pesquisa dos profissionais dessa área durante algumas décadas, elegendo-a, assim, como um padrão seguido de maneira mundial. Seu principal objetivo é a elaboração de práticas, implantadas, testadas e aprovadas pelas organizações, que serão posteriormente utilizadas por elas.

Os conceitos teóricos dos principais componentes da ITIL (estratégia de serviço, desenho de serviço, transição de serviço, operação de serviço e melhoria de serviço continuada), bem como dois modelos de melhores práticas, serão apresentados detalhadamente na Unidade 5.

Por fim, desejamos a você um ótimo trabalho e sucesso nos seus estudos.

Glossário de Conceitos

O Glossário de Conceitos permite a você uma consulta rápida e precisa das definições conceituais, possibilitando-lhe um bom domínio dos termos técnico-científicos utilizados na área de conhecimento dos temas tratados em *Segurança e Auditoria de Sistemas*. Veja, a seguir, a definição dos principais conceitos:

1) **Análise de risco**: na TI, trata-se do processo de estudo preliminar dos riscos a que estão sujeitos os sistemas computacionais. Essa análise é utilizada posteriormente para desenvolvimento de uma política de segurança específica para a organização.
2) **Assinatura digital**: "é um conjunto de operações criptográficas aplicadas a um determinado arquivo" (PORTAL DA JUSTIÇA FEDERAL, 2011). É um mecanismo que foi desenvolvido com o objetivo de proteger a informação e assegurar sua transmissão de modo seguro. Atua na autenticação da informação digital.
3) **Auditoria**: "uma auditoria é uma revisão das demonstrações financeiras, sistema financeiro, registros, transações e operações de uma entidade ou de um projeto, efetuada por contadores, com a finalidade de assegurar a fidelidade dos registros e proporcionar credibilidade às demonstrações financeiras e outros relatórios da administração" (PORTAL DE CONTABILIDADE, 2011).
4) ***Balanced scorecard***: de acordo com Kaplan e Norton (1997), é um método que busca esclarecer, comunicar e alinhar a estratégia à organização, por meio da tradu-

ção da visão, missão e estratégia das empresas em um conjunto abrangente de objetivos e medidas de desempenho tangíveis que servem de base para sistemas de medição.

5) **COBIT (*Control Objectives for Information and Related Technology*)**: pode ser definido como um modelo de padrões internacionais de boas práticas focado na gestão e na auditoria de tecnologia.

6) **Computação quântica**: é um domínio de pesquisa recente que utiliza elementos de três áreas bem conhecidas: Matemática, Física e Computação. Sua vantagem sobre a computação clássica é a velocidade de processamento dos dados, ou seja, seu tempo de resposta.

7) **DDoS**: é uma derivação do ataque DoS. "O ataque DDoS é dado, basicamente, em três fases: uma fase de 'intrusão em massa', na qual ferramentas automáticas são usadas para comprometer máquinas e obter acesso privilegiado (acesso de root). Outra, onde o atacante instala *software* DDoS nas máquinas invadidas com o intuito de montar a rede de ataque. E, por último, a fase onde é lançado algum tipo de flood de pacotes contra uma ou mais vítimas, consolidando efetivamente o ataque" (REDE NACIONAL DE ENSINO E PESQUISA, 2011).

8) **DoS (*Denial of Service*)**: trata-se de um ataque de negação de serviço, ou seja, uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores.

9) **Endereço MAC (*Media Access Control*)**: trata-se do endereço físico de 48 *bits* da interface de rede. É o endereço de controle de acesso da placa de rede.

10) **Engenharia social**: são práticas utilizadas para obtenção de acesso a informações confidenciais de organizações ou particulares, por meio da enganação ou exploração da confiança das pessoas. Desse modo, um indivíduo mal-intencionado poderá fingir ser outra pessoa, como, por exemplo, assumir outra personalidade e, até mesmo, se apresentar como um profissional de uma determinada área. Sendo assim, trata-se de uma forma de en-

trar nas organizações sem o uso de força bruta, ou seja, as técnicas utilizadas contam com as falhas de segurança das pessoas que atuam diretamente nos sistemas de informação.

11) ***Firewall***: "um firewall evita que perigos vindos da internet espalhem-se na sua rede interna. Colocado entre a rede interna e a externa, o firewall controla todo o tráfego que passa entre elas, tendo a certeza que este tráfego é aceitável, de acordo com a política de segurança do site, oferecendo uma excelente proteção contra ameaças vindas da rede externa" (REDE NACIONAL DE ENSINO E PESQUISA, 2011).
12) **Função *hash***: é uma função que comprime ou resume os dados em um número fixo de *bits*, a partir de uma sequência de tamanho variado. Assim, proteger o resultado *hash* torna-se mais fácil do que proteger a mensagem inteira. A assinatura digital faz uso de funções *hash*.
13) ***Gateway***: também conhecido como "porta de entrada", é utilizado normalmente para interligação entre duas redes. Disponível em forma de *hardware* dedicado ou de um computador com duas ou mais interfaces de rede.
14) ***Hacker***: pessoa que desenvolve e/ou altera *softwares* e/ou *hardwares* de computadores.
15) **ITIL (*Information Technology Infrastructure Library*)**: é a abordagem mais amplamente adotada para o gerenciamento de serviços de TI no mundo. Fornece uma forma prática para a identificação, o planejamento, a entrega e o suporte de serviços de TI para o negócio (ITIL, 2011).
16) ***Passphrase* (frase-chave)**: é uma sequência de palavras ou outro texto usado para controlar o acesso a um sistema de computador, programa ou dados.
17) ***Phishing***: "o conjunto de técnicas empregadas para roubar a Identidade Eletrônica de um indivíduo, permitindo o acesso a áreas ou serviços privados em benefício próprio constitui delito de fraude" (INTERNET SEGURA, 2011).
18) **Política de segurança**: é a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos

da empresa. A partir do estudo ou análise de risco de determinada organização, os profissionais que atuam nas áreas de segurança da informação devem ser capazes de desenvolver uma política de segurança específica que atenda às necessidades pontuais dessa organização. A política de segurança deve descrever as regras de forma clara e objetiva, como também deve estar alinhada com a política de estratégia da empresa. Uma vez divulgada amplamente, a política deve ser cumprida por todos, e as punições devem ser aplicadas nos casos em que não for respeitada.

19) **Protocolo WEP (*Wired Equivalent Privacy*)**: é um algoritmo de segurança para redes sem fio (IEEE 802.11). Sua função é fornecer confidencialidade de dados comparável à de uma rede com fio tradicional.
20) **Protocolo WPA (Wi-Fi *Protected Access*)**: é um protocolo de segurança desenvolvido pela Wi-Fi Alliance para proteger redes de computadores sem fio.
21) **Segurança da informação**: cada organização define seus níveis de acesso, que variam desde a simples permissão de acesso a arquivos até a elaboração de uma complexa definição de segurança, permitindo acesso a dados ou serviços específicos e restringindo áreas consideradas confidenciais. São diversos os aspectos que definem a importância da segurança em sistemas computacionais, porém todos buscam em conjunto garantir a segurança da informação da organização. Independentemente das escolhas, é importante manter o foco no objetivo, que é a busca de mecanismos eficazes que diminuam as vulnerabilidades das informações e que se mantenham funcionais com o decorrer do tempo.
22) **Servidor *proxy***: é um servidor como um aplicativo (*software*) que atua de forma semelhante a um intermediário para solicitações de clientes que procuram recursos de outros servidores.
23) **SSID (*Service Set Identifier*)**: é um nome que identifica uma determinada rede sem fio.

24) ***Three-way handshaking***: mecanismo de estabelecimento de conexão em três tempos que permite a autenticação de uma sessão.

Esquema dos Conceitos-chave

Para que você tenha uma visão geral dos conceitos mais importantes deste estudo, apresentamos, a seguir (Figura 1), um Esquema dos Conceitos-chave. O mais aconselhável é que você mesmo faça o seu esquema de conceitos-chave ou até mesmo o seu mapa mental. Esse exercício é uma forma de você construir o seu conhecimento, ressignificando as informações a partir de suas próprias percepções.

É importante ressaltar que o propósito desse Esquema dos Conceitos-chave é representar, de maneira gráfica, as relações entre os conceitos por meio de palavras-chave, partindo dos mais complexos para os mais simples. Esse recurso pode auxiliar você na ordenação e na sequenciação hierarquizada dos conteúdos de ensino.

Com base na teoria de aprendizagem significativa, entende-se que, por meio da organização das ideias e dos princípios em esquemas e mapas mentais, o indivíduo pode construir o seu conhecimento de maneira mais produtiva e obter, assim, ganhos pedagógicos significativos no seu processo de ensino e aprendizagem.

Aplicado a diversas áreas do ensino e da aprendizagem escolar (tais como planejamentos de currículo, sistemas e pesquisas em Educação), o Esquema dos Conceitos-chave baseia-se, ainda, na ideia fundamental da Psicologia Cognitiva de Ausubel, que estabelece que a aprendizagem ocorre pela assimilação de novos conceitos e de proposições na estrutura cognitiva do aluno. Assim, novas ideias e informações são aprendidas, uma vez que existem pontos de ancoragem.

Tem-se de destacar que "aprendizagem" não significa, apenas, realizar acréscimos na estrutura cognitiva do aluno; é preciso, sobretudo, estabelecer modificações para que ela se configure como uma aprendizagem significativa. Para isso, é importante considerar as entradas de conhecimento e organizar bem os materiais de aprendizagem. Além disso, as novas ideias e os novos conceitos devem ser potencialmente significativos para o aluno, uma vez que, ao fixar esses conceitos nas suas já existentes estruturas cognitivas, outros serão também relembrados.

Nessa perspectiva, partindo-se do pressuposto de que é você o principal agente da construção do próprio conhecimento, por meio de sua predisposição afetiva e de suas motivações internas e externas, o Esquema dos Conceitos-chave tem por objetivo tornar significativa a sua aprendizagem, transformando o seu conhecimento sistematizado em conteúdo curricular, ou seja, estabelecendo uma relação entre aquilo que você acabou de conhecer com o que já fazia parte do seu conhecimento de mundo (adaptado do *site* disponível em: <http://penta2.ufrgs.br/edutools/mapasconceituais/utilizamapasconceituais.html>. Acesso em: 11 mar. 2010).

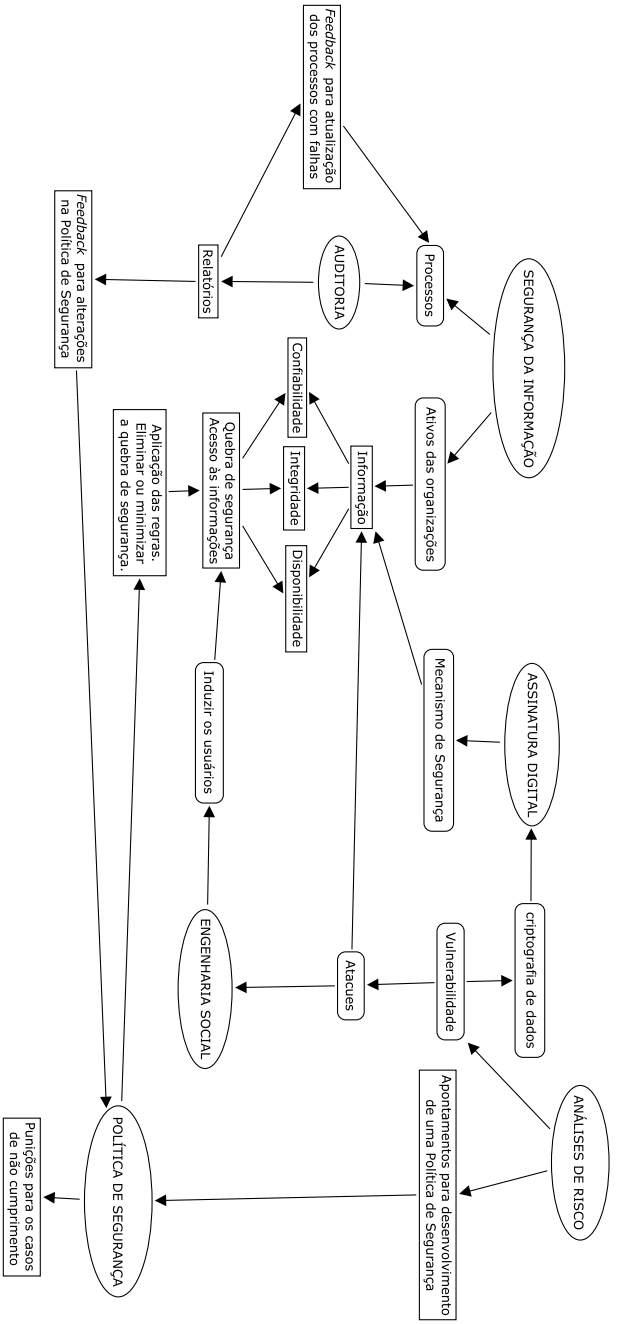


Figura 1 *Esquema dos Conceitos-chave do Caderno de Referência de Conteúdo de Segurança e Auditoria de Sistemas*.

Como pode observar, esse esquema oferece a você, como dissemos anteriormente, uma visão geral dos conceitos mais importantes deste estudo. Ao segui-lo, será possível transitar entre os principais conceitos e descobrir o caminho para construir o seu processo de ensino-aprendizagem. Por exemplo, o conceito de **política de segurança** implica o conhecimento da **análise de riscos**, como também dos apontamentos produzidos por tal análise. Somente após compreender esse conceito o estudo da política se tornará mais claro.

O Esquema dos Conceitos-chave é mais um dos recursos de aprendizagem que vem se somar àqueles disponíveis no ambiente virtual, por meio de suas ferramentas interativas, bem como àqueles relacionados às atividades didático-pedagógicas realizadas presencialmente no polo. Lembre-se de que você, aluno EaD, deve valer-se da sua autonomia na construção de seu próprio conhecimento.

Questões Autoavaliativas

No final de cada unidade, você encontrará algumas questões autoavaliativas sobre os conteúdos ali tratados, as quais podem ser de **múltipla escolha**, **abertas objetivas** ou **abertas dissertativas**.

Responder, discutir e comentar essas questões, bem como relacioná-las com a prática de segurança e auditoria de sistemas, pode ser uma forma de você avaliar o seu conhecimento. Assim, mediante a resolução de questões pertinentes ao assunto tratado, você estará se preparando para a avaliação final, que será dissertativa. Além disso, essa é uma maneira privilegiada de você testar seus conhecimentos e adquirir uma formação sólida para a sua prática profissional.

Você encontrará, ainda, no final de cada unidade, um gabarito que lhe permitirá conferir as suas respostas sobre as questões autoavaliativas de múltipla escolha.

As **questões de múltipla escolha** são as que têm como resposta apenas uma alternativa correta. Por sua vez, entendem-se por **questões abertas objetivas** as que se referem aos conteúdos matemáticos ou àqueles que exigem uma resposta determinada, inalterada. Já as **questões abertas dissertativas** obtêm por resposta uma interpretação pessoal sobre o tema tratado; por isso, normalmente, não há nada relacionado a elas no item Gabarito. Você pode comentar suas respostas com o seu tutor ou com seus colegas de turma.

Bibliografia Básica

É fundamental que você use a Bibliografia Básica em seus estudos, mas não se prenda só a ela. Consulte, também, as bibliografias complementares.

Figuras (ilustrações, quadros...)

Neste material instrucional, as ilustrações fazem parte integrante dos conteúdos, ou seja, elas não são meramente ilustrativas, pois esquematizam e resumem conteúdos explicitados no texto. Não deixe de observar a relação dessas figuras com os conteúdos, pois relacionar aquilo que está no campo visual com o conceitual faz parte de uma boa formação intelectual.

Dicas (motivacionais)

Este estudo convida você a olhar, de forma mais apurada, a Educação como processo de emancipação do ser humano. É importante que você se atente às explicações teóricas, práticas e científicas que estão presentes nos meios de comunicação, bem como partilhe suas descobertas com seus colegas, pois, ao compartilhar com outras pessoas aquilo que você observa, permite-se descobrir algo que ainda não se conhece, aprendendo a ver e a notar o que não havia sido percebido antes. Observar é, portanto, uma capacidade que nos impele à maturidade.

Você, como aluno dos Cursos de Graduação na modalidade EaD, necessita de uma formação conceitual sólida e consistente. Para isso, você contará com a ajuda do tutor a distância, do tutor presencial e, sobretudo, da interação com seus colegas. Sugerimos, pois, que organize bem o seu tempo e realize as atividades nas datas estipuladas.

É importante, ainda, que você anote as suas reflexões em seu caderno ou no Bloco de Anotações, pois, no futuro, elas poderão ser utilizadas na elaboração de sua monografia ou de produções científicas.

Leia os livros da bibliografia indicada, para que você amplie seus horizontes teóricos. Coteje-os com o material didático, discuta a unidade com seus colegas e com o tutor e assista às videoaulas.

No final de cada unidade, você encontrará algumas questões autoavaliativas, que são importantes para a sua análise sobre os conteúdos desenvolvidos e para saber se estes foram significativos para sua formação. Indague, reflita, conteste e construa resenhas, pois esses procedimentos serão importantes para o seu amadurecimento intelectual.

Lembre-se de que o segredo do sucesso em um curso na modalidade a distância é participar, ou seja, interagir, procurando sempre cooperar e colaborar com seus colegas e tutores.

Caso precise de auxílio sobre algum assunto relacionado a este *Caderno de Referência de Conteúdo*, entre em contato com seu tutor. Ele estará pronto para ajudar você.

3. E-REFERÊNCIAS

INTERNET SEGURA. *Phishing*. Disponível em: <http://www.internetsegura.org/nsegura/phising.asp>. Acesso em: 27 set. 2011.

ITI – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. *Publicações do ITI*. Cartilhas Certificação Digital. O que é certificação digital?. Disponível em: <http://www.

iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>. Acesso em: 3 jul. 2011.

ITIL. *What is ITIL?*. Disponível em: <http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx>. Acesso em: 5 jul. 2011.

PORTAL DA JUSTIÇA FEDERAL. *O que é assinatura digital*. Disponível em: <http://www.jf.jus.br/cjf/tecnologia-da-informacao/identidade-digital/o-que-e-assinatura-digital>. Acesso em: 26 set. 2011.

PORTAL DE CONTABILIDADE. *Auditoria*. Conceito. Objetivos. Disponível em: <http://www.portaldecontabilidade.com.br/guia/auditoria.htm>. Acesso em: 26 set. 2011.

REDE NACIONAL DE ENSINO E PESQUISA. *Firewalls*. Disponível em: <http://www.rnp.br/newsgen/9708/n3-1.html#ng-introducao>. Acesso em: 27 set. 2011.

_____. *Tudo que você precisa saber sobre os ataques DdoS*. Disponível em: <http://www.rnp.br/newsgen/0003/ddos.html>. Acesso em: 27 set. 2011.

TREND MICRO. *Phishing*. Disponível em: <http://br.trendmicro.com/br/threats/home-user/common-threats/phishing/>. Acesso em: 5 jul. 2011.

4. REFERÊNCIAS BIBLIOGRÁFICAS

FERNANDES, A. A.; ABREU, V. F. *Implantando a Governança de TI*: da estratégia à gestão dos processos e serviços. 2. ed. Rio de Janeiro: Brasport, 2008.

KAPLAN, R. S.; NORTON D. P. *A estratégia em ação*: balanced scorecard. 7. ed. Rio de Janeiro: Campus, 1997.

EAD

Introdução à Segurança e à Auditoria de Sistemas

1

1. OBJETIVOS

- Caracterizar problemas de segurança.
- Avaliar o risco e seu impacto.
- Descrever política de segurança e técnicas utilizadas para aumento da segurança.

2. CONTEÚDOS

- Aspectos de segurança.
- Análise de riscos.
- Política de segurança.

3. ORIENTAÇÕES PARA O ESTUDO DA UNIDADE

Antes de iniciar o estudo desta unidade, é importante que você leia as orientações a seguir:

1) Esta unidade versará sobre os principais aspectos de segurança de um sistema de informação, que servirão de base para o estudo e o entendimento das demais unidades deste *Caderno de Referência de Conteúdo*. Além disso, tratará da análise de riscos e das características essenciais de uma política de segurança. Portanto, é essencial que você atente aos conceitos apresentados e não deixe que restem dúvidas ao final do estudo.
2) Observe e anote as palavras-chave, buscando sua compreensão antes de prosseguir com a leitura, para o pleno aprendizado dos conceitos abordados na unidade. Também verifique o significado dos termos apresentados no Glossário de Conceitos, buscando relacioná-los com o Esquema dos Conceitos-chave para aplicação no estudo de todas as unidades deste *Caderno de Referência de Conteúdo* (CRC). Essas práticas buscam facilitar o processo de aprendizagem.
3) Leia os livros indicados na bibliografia, buscando ampliar seus conhecimentos teóricos. Interaja com seus colegas e com seu tutor.
4) Proponha-se a elaborar uma política de segurança simples. Busque conhecer modelos já elaborados e implementados nas organizações. Por meio da familiarização criada no contato direto com esses materiais, você terá maior facilidade para desenvolver suas próprias políticas de segurança.
5) Complemente seu conhecimento realizando a leitura de *Pequeno histórico sobre o surgimento das normas de segurança de autoria*, de Luís Rodrigo de Oliveira Gonçalves, disponível em: <http://www.batori.com.br/pag__con.asp?id_pagina=448>. Acesso em: 27 set. 2011.
6) Você poderá obter mais informações sobre as normas específicas de segurança da informação acessando as normas ISO/IEC 27001:2005 (*Information Technology – Security Techniques – Information Security Management Systems – Requirements*) e ISO/IEC 29192-1:2012 (*Information Technology – Security Techniques – Lightweight Cryptography – Part 1: General*) na íntegra. Ambas as normas citadas, bem como as

demais relacionadas à segurança da informação, estão disponíveis no endereço: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306>. Acesso em: 12 maio 2012.

4. INTRODUÇÃO À UNIDADE

Nesta primeira unidade, você estudará os principais aspectos de segurança presentes em um sistema, destacando o papel da informação como elemento importante para a geração de conhecimento, a tomada de decisões e, principalmente, o valor que agrega ao negócio.

No início, os sistemas trabalhavam isoladamente, e os riscos de ataques estavam sujeitos a atividades internas das corporações, facilitando, assim, sua identificação e resolução. Atualmente, os ataques podem partir de qualquer parte do mundo. Basta analisarmos o conceito de "computação em nuvem" (*cloud computing*), em que os recursos disponíveis, como processamento, memória e outros, são compartilhados por meio da internet.

Assim, a análise de risco e o desenvolvimento de uma política de segurança são fatores fundamentais para obtenção de um sistema de informação seguro.

Afinal, o que é um sistema seguro?

Sua resposta deverá ser o seu motivador para o estudo deste *Caderno de Referência de Conteúdo*.

Vejamos, a seguir, os aspectos de segurança.

5. ASPECTOS DE SEGURANÇA

O bem mais valioso de uma empresa talvez não seja seus produtos e serviços, mas as informações que, de uma maneira ou outra, estejam relacionadas com eles.

A maneira de registrar as informações sofre mudanças desde a Pré-história, período no qual as informações ficavam restritas basicamente ao armazenamento na memória humana. Posteriormente, elas foram gravadas nas paredes das habitações, o que as tornava acessíveis, e, ao mesmo tempo, não era possível sua mobilidade.

Já no final da Idade Média, as informações tornaram-se portáveis, com o surgimento da tecnologia de impressão. Hoje, criou-se uma dependência em relação à tecnologia das informações e da comunicação, nascida da necessidade de implementações de segurança da informação, para que ela esteja disponível, íntegra e restrita, isto é, seja acessada somente a quem tem direito.

Atualmente, em consequência dos avanços tecnológicos, principalmente na área da Informática, a segurança de acesso lógico tornou-se necessária, ou seja, as ferramentas de controle são implementadas nos ambientes computacionais e geralmente só serão notadas pelos usuários quando tiverem o seu acesso negado a algum recurso.

O controle de acesso lógico mais comum é baseado no uso de senhas para autenticação de usuários. Os acessos são controlados por listas de acesso que determinam para cada usuário os recursos que poderão ser acessados e, também, seus níveis de acesso dentro desses recursos.

Devemos compreender o significado do termo "acesso lógico" como o acesso ao ambiente de informações ou ao conteúdo informacional, mais frequentemente associado à informática, mas que também pode ser aplicado a informações restritas de uma organização que não estejam armazenadas dentro dos seus sistemas computacionais.

Os ativos de informações de uma organização apresentam um relacionamento com alguns agentes, como, por exemplo, o agente proprietário, custo diante, usuário e o agente controlador – esse último, conforme já estudado, age no controle dos acessos ao ativo propriamente dito.

A propriedade sobre os ativos de informações das organizações foi transferida da área de informática para o usuário final. A área de Tecnologia da Informação é custo diante dos ativos de informações dos usuários, bem como guarda e processa tais ativos em nome dos seus legítimos proprietários.

O profissional em segurança de sistemas deve ser capaz de identificar em que local a segurança se faz indispensável, como também ponderar sobre os investimentos necessários.

Cada organização define seus níveis de acesso, que variam desde a simples permissão para arquivos até a elaboração de uma complexa definição de segurança, de modo que permita acesso a dados ou serviços específicos e restrinja em áreas consideradas confidenciais.

São diversos os aspectos que definem a importância da segurança em sistemas computacionais, porém todos buscam garantir a segurança da informação da organização.

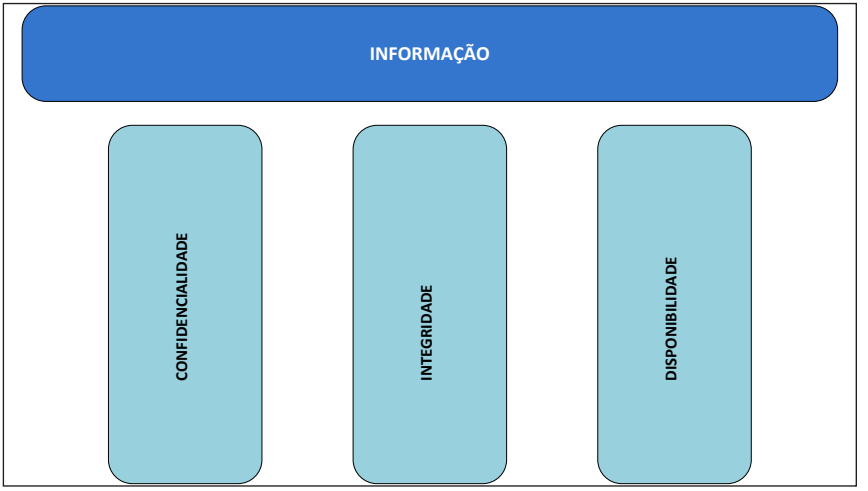
Os incidentes de segurança da informação, isto é, quando uma informação deixa de ser confidencial, íntegra ou disponível quando necessária, podem causar prejuízos à organização, como desgaste da sua imagem e perdas financeiras.

É preciso que os recursos, muitas vezes limitados, sejam bem administrados, uma vez que as inúmeras possibilidades tornam confuso o cenário de decisão. Surgem alguns questionamentos, tais como:

- Adquirir uma nova ferramenta de antivírus?
- Investir em treinamentos de segurança?

Independentemente da decisão tomada, é importante manter o foco no objetivo, que é a busca por mecanismos eficazes que diminuam as vulnerabilidades das informações e que continuem funcionais com o decorrer do tempo.

Observe, na Figura 1, os principais aspectos de um sistema de segurança da informação.



Fonte: Campos (2007, p. 17).
Figura 1 *Características de segurança da informação*.

Confidencialidade dos dados

A confidencialidade dos dados refere-se à proteção contra o acesso não autorizado a eles. Seus objetivos são atingidos quando a informação é somente acessada por pessoas autorizadas.

A partir do momento em que uma pessoa não autorizada tem acesso a determinada informação, está caracterizado um incidente de segurança da informação por quebra de confidencialidade. Esse acesso indevido pode ser intencional ou não.

A quebra de confidencialidade não ocorre somente em ambientes corporativos, pois os dados armazenados em computadores pessoais também são passíveis de tentativas de acesso por pessoas não autorizadas. É nesse cenário que pessoas mal-intencionadas utilizam técnicas a fim de obter tais informações, como, por exemplo, a engenharia social.

Conforme definição do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – CERT.br (2011):

> Nos ataques de engenharia social, normalmente, o atacante se faz passar por outra pessoa e utiliza meios, como uma ligação telefônica ou *e-mail*, para persuadir o usuário a fornecer informações ou realizar determinadas ações. Exemplos destas ações são: executar um programa, acessar uma página falsa de comércio eletrônico ou *Internet Banking* através de um *link* em um *e-mail* ou em uma página etc.

A fim de evitar tais incidentes, estudaremos, nas unidades seguintes, alguns mecanismos, como sistemas de detecção de intruso, controle de acesso lógico e assinatura digital, entre outros.

Integridade dos dados

A integridade dos dados está relacionada à proteção contra a alteração dos dados. A integridade é atingida quando a informação é mantida íntegra.

Quando uma pessoa não autorizada altera ou corrompe a informação, caracteriza-se um incidente de segurança da informação por quebra de integridade. Por exemplo, os dados armazenados em um banco de dados devem ter sua integridade garantida para que sejam transformados em informação, ou seja, sem essa garantia, certamente não conseguiremos transformar esses *bytes* em informação útil.

Disponibilidade de dados

A disponibilidade de dados trata-se de um aspecto de proteção contra a interrupção do acesso a dados ou serviços. Seus objetivos são alcançados quando a informação estiver acessível sempre que pessoas autorizadas necessitarem. A indisponibilidade a dados ou serviços caracteriza um incidente de segurança da informação por quebra de disponibilidade.

Imagine que o serviço de *e-mail* por algum motivo deixe de funcionar. Mesmo que não seja fruto de uma invasão intencional,

esse incidente provavelmente causará aos usuários, no mínimo, a sensação de descontentamento pela indisponibilidade do serviço e, em muitos casos, o cancelamento do serviço por falta de segurança.

Em contrapartida, podemos avaliar os prejuízos causados quando um incidente dessa natureza ocorre com o serviço considerado fundamental para a organização, como é o caso do comércio eletrônico (*e-commerce*). Caso um portal de vendas pela internet fique indisponível, além dos prejuízos financeiros originados pela não comercialização durante esse período, a imagem da organização será afetada perante seus clientes, podendo vir a inibir futuras transações.

Quando tratamos de segurança da informação, não podemos deixar de lado as questões relacionadas ao direito de acesso dos usuários. Nesse cenário, existem alguns requisitos que regulam o direito de acesso aos recursos nas organizações, como, por exemplo, a proteção de ativos, práticas de auditoria e legislações.

Vamos falar um pouco mais sobre legislação?

É sabido que, em alguns países, existem leis cujo objetivo é regular as responsabilidades dos administradores e usuários de recursos de informações. Porém, em outros países, tais dispositivos legais ainda não foram implantados e talvez nem discutidos.

Apesar desse cenário heterogêneo, os administradores de organizações multinacionais devem se atentar para a legislação específica do país sede da empresa. Por exemplo, no caso das leis norte-americanas, são responsabilizados os administradores de recursos que atuam em suas filiais pela segurança das informações.

Algumas leis – principalmente as dos Estados Unidos – podem ser aplicadas a empresas norte-americanas em outros países e a empresas estrangeiras com filiais nos Estados Unidos, como também a empresas que disponham de títulos comercializados

em bolsas de valores americanas. Ainda nesse cenário, podemos citar a Lei Sarbanes-Oxley, que engloba aspectos mais específicos desse tipo de legislação. Observe, a seguir, o que trata essa lei.

Lei Sarbanes-Oxley

A Lei Sarbanes-Oxley foi promulgada em 2002 com o objetivo de melhorar a precisão e a confiabilidade das informações divulgadas pelas organizações, em obediência às leis de segurança da informação. Ela exige que as empresas implementem uma organização interna de controle e procedimentos para elaboração de relatórios financeiros coerentes, como também prevê as penalidades a que estão sujeitos os membros da alta direção da empresa.

A referida lei obriga a prática de um novo nível de governança e responsabilização por parte das organizações, ou seja, elas terão de incluir suas estruturas de gestão e monitoramento de registros e avaliação de vulnerabilidades em suas ferramentas de controle interno de Tecnologia da Informação (TI).

As regras são válidas – como citado anteriormente – para empresas norte-americanas, como também para empresas multinacionais que possuam ações (papéis) negociadas em bolsas americanas, como, por exemplo, a Nasdaq. Enfim, todas devem obedecer à Lei Sarbanes-Oxley.

De acordo com Caruso e Steffen (2006), isso implica métodos e trilhas de auditoria e registros de possíveis alterações de registros eletrônicos, conforme exigido no Artigo 404 dessa lei.

As adequações às exigências por parte das empresas dão-se por meio do estabelecimento de alguns controles:

1) **Controle de acesso**: monitora todas as tentativas de acesso a sistemas de relatórios financeiros.
2) **Controle de configuração**: monitora a configuração, políticas e *softwares* instalados.
3) **Detecção de *software* malicioso**: coleta e transmite informações sobre atividades maliciosas.

4) **Verificação da obediência à política**: monitora a obediência da lei por parte de todos os usuários.
5) **Monitoramento e gerenciamento de usuários**: realiza uma auditoria completa de atividades por parte de terceiros que possuam acesso a dados sensíveis.
6) **Segurança de ambiente e de divulgação**: monitora o ambiente, garantindo a identificação e correção de riscos relativos à segurança.

Veremos, agora, a análise de riscos.

6. ANÁLISE DE RISCOS

Para gerenciar a segurança da informação de modo efetivo, devemos trabalhar, inicialmente, na identificação e análise dos riscos de incidentes de segurança, os quais já foram abordados anteriormente.

Conforme salienta Campos (2007, p. 50):

> A análise de risco possibilita identificar o grau de proteção de que os ativos de informação de cada processo da organização precisam, permitindo assim não apenas proporcionar a proteção em grau adequado para o negócio, mas principalmente usar de maneira inteligente os recursos da organização.

Os objetivos da análise de riscos são coletar informações sobre o grau de segurança existente em determinado ambiente da organização e elaborar um plano de segurança, que estudaremos mais adiante.

Alguns dos fatores característicos de ameaças são apresentados na Tabela 1.

Tabela 1 Riscos que ameaçam os ativos de informações.

CAMPOS DE RISCO	AMEAÇAS (EXEMPLOS)
Local/edifício	Fogo, raios, água, furtos/roubos, espionagem, terrorismo/sabotagem.

CAMPOS DE RISCO	AMEAÇAS (EXEMPLOS)
Infraestrutura técnica	Insuficiência de equipamentos, falhas técnicas, oscilações elétricas, falta de energia/água/combustível.
Redes de comunicação	Sabotagem, espionagem, modificações, fraudes, quedas/interrupções.
Software	Furtos, alterações indevidas, vírus, falta de controle de acesso.
Dados/meios de armazenamento	Falhas de controle, *backups* insuficientes/ inadequados, desmagnetização, falhas no transporte, falhas no armazenamento.
Hardware	Oscilações de energia, falhas de climatização, instalações inadequadas, danos físicos.

Fonte: adaptado de Caruso e Steffen (2006, p. 72).

Como podemos observar na tabela, existem várias formas de ameaças aos ativos de informações. Uma vez segmentados os campos de riscos, torna-se mais fácil identificar suas respectivas ameaças, bem como elaborar posteriormente procedimentos para combatê-las. Por exemplo, identificada uma ameaça de vírus, o plano de segurança deve apresentar os procedimentos cabíveis para evitar ou impedir tais ocorrências.

A segurança de ativos de informações deve atingir seu objetivo principal, porém, como em quase todas as áreas, existem algumas restrições. Nesse caso, deve ser considerada a relação custo/benefício de sua implementação, como também a prática do bom senso nas decisões.

Como podemos perceber, a tarefa de identificar os riscos e implementar a segurança não é um processo simples. A Figura 2 apresenta uma proposta para o fluxo de análise das ameaças e riscos.

Fonte: Caruso e Steffen (2006, p. 73).
Figura 2 *Fluxo de análise das ameaças e riscos*.

O fluxo apresentado pela Figura 2 propõe uma metodologia simples que auxilie nas tomadas de decisão dos investimentos em segurança por meio da relação entre as ameaças e os riscos. Essa metodologia pode ser descrita da seguinte maneira:

1) São realizadas a análise dos riscos e suas consequências.
2) São estimadas as probabilidades de tais ocorrências.
3) São atribuídos o peso ou o dano causado pela ocorrência.
4) É calculada a exposição ao risco: E = V x P, onde V representa a vulnerabilidade ou dano e P, a probabilidade da ocorrência em vezes/ano.
5) São analisadas as medidas de proteção aos riscos.
6) São escolhidas as medidas de proteção a se empregar, de acordo com a relação custo/eficácia da segurança.

Uma vez compreendida a análise de risco, os riscos deverão ser avaliados. Quais serão os critérios de validação?

A resposta para tal questão está na elaboração do que chamamos de "estratégia de avaliação de risco". Essa é a etapa inicial da análise de risco, que busca definir diretrizes para que os resultados esperados sejam alcançados.

Campos (2007, p. 52) ressalta que "[...] os investimentos em diminuição dos riscos não devem exceder a 1% do faturamento da organização".

Neste *Caderno de Referência de Conteúdo*, trabalharemos com a análise de risco em qualitativa. Entre outras formas de análise, a análise qualitativa destaca-se, pois aborda aspectos mais superficiais, e os resultados são obtidos mais facilmente, porém apresenta resultados menos exatos. Seja qual for o método utilizado, a ameaça, a vulnerabilidade e o impacto devem ser considerados, a fim de se obter uma base de risco. Vejamos.

Ameaças

As ameaças devem ser classificadas em relação ao grau de exposição apresentado, ou seja, quanto maior for seu grau de exposição, maiores serão sua probabilidade e vulnerabilidade. Um exemplo de classificação por grau de exposição é ilustrado na Tabela 2.

Tabela 2 Classificação de ameaças.

AMEAÇA		
GRAU DE EXPOSIÇÃO	VALOR REFERENCIAL	FAIXA (%)
Baixo	1	0-25
Médio	2	26-70
Alta	3	71-100

Analisando o exemplo apresentado na Tabela 2, foram definidos três níveis de grau de exposição: baixo, médio e alto. Quanto maior a quantidade de níveis estabelecidos, mais bem definidas serão as faixas de classificação. Nesse caso, uma ameaça que apresente grau de exposição médio foi categorizada na faixa entre 26% e 70%, ou seja, nessa faixa, foram agrupadas ameaças que, por exemplo, representem prejuízos da ordem de 26% a 70% de um valor preestabelecido. O valor referencial, nesse caso, é só uma maneira simplificada de referenciar as faixas propostas.

Os dados da 10ª Pesquisa Nacional de Segurança da Informação, realizada em 2006, pela empresa Módulo – *Technology for Risk Management*, revelam as principais ameaças geradoras de perdas financeiras. As informações oficiais servem como indicadores para elaboração de uma política de segurança, conforme demonstrado na Figura 3.

Figura 3 *Resultado da 10ª Pesquisa Nacional de Segurança da Informação (2006)*.

Ao analisarmos a Figura 3, podemos notar uma grande variedade de tipos de ataque, que, se não forem tratados por uma política de segurança, podem gerar prejuízos à organização, como falhas na segurança física, que representam 7% dessas ocorrências.

Vulnerabilidade

A vulnerabilidade deve ser classificada em relação ao grau de vulnerabilidade para cada ameaça, uma vez que ela varia conforme a ameaça apresentada. Um exemplo dessa classificação é ilustrado na Tabela 3.

Tabela 3 Classificação de vulnerabilidade.

VULNERABILIDADE		
DEFICIÊNCIA DE CONTROLES	VALOR REFERENCIAL	FAIXA (%)
Baixa	1	0-25
Média	2	26-70
Alta	3	71-100

Impacto

Por fim, temos o indicador de impacto, o qual pode ser mensurado de várias maneiras, porém, para fins didáticos, neste material, utilizaremos o exemplo do grau de impacto *versus* duração de interrupção suportada de um determinado serviço. Veja a ilustração na Tabela 4.

Tabela 4 Classificação de impacto.

IMPACTO		
INTERRUPÇÃO	VALOR REFERENCIAL	FAIXA (%)
Baixa (30 dias)	1	0-25
Média (10 dias)	2	26-70
Alta (1 dia)	3	71-100

Mesmo depois de identificadas todas as ameaças por meio da análise de riscos, nem sempre é viável a implementação de segurança em todas as vulnerabilidades apontadas, visto que devemos também levar em conta a relação custo/benefício, isto é, os investimentos em segurança não devem ultrapassar o valor do ativo a ser protegido, conforme citado anteriormente. Claro que, para cada caso, cabe uma análise pontual, e as decisões devem ser tomadas com bom senso.

Por meio da análise de riscos, os profissionais em segurança de sistemas dispõem dos subsídios necessários para elaboração de uma política de segurança eficaz, baseada nos indicadores de vulnerabilidade e impacto de maior relevância.

Iniciaremos, a seguir, o estudo da política de segurança.

7. POLÍTICA DE SEGURANÇA

A política de segurança abrange os controles que, uma vez implementados, buscam diminuir as vulnerabilidades do sistema de informação. Deve ser amplamente divulgada para que todos na organização a conheçam, bem como deve apresentar as penalidades às quais estão sujeitos aqueles que não a cumprirem.

Conforme define Caruso (1999, p. 24):

> Por política de segurança entende-se política elaborada, implementada e em contínuo processo de revisão, válida para toda organização, com regras o mais claras e simples possível e estrutura gerencial e material de suporte a essa política, claramente sustentada pela alta hierarquia.

Espera-se, a partir de uma política de segurança corretamente implementada, atingir os seguintes objetivos:

- Diminuir a probabilidade de ocorrência.
- Diminuir os prejuízos causados por eventuais ocorrências.
- Elaborar procedimentos para recuperação de desastres.

A seguir, analisaremos cada um dos objetivos apresentados.

Diminuir a probabilidade de ocorrência

Quando falamos em diminuir a probabilidade de ocorrência, queremos dizer que as ameaças devem ser previamente identificadas e tratadas, isto é, espera-se que as ameaças sejam eliminadas antes que ocorram. O caráter preventivo dessa ação normalmente demanda menos esforços (técnicos, financeiros, entre outros) do que as ações de recuperação de desastres causadas por falta de segurança.

Diminuir os prejuízos causados por eventuais ocorrências

Se mesmo com a aplicação das medidas preventivas ocorre algum tipo de incidente de segurança, os impactos devem ser diminuídos. A tarefa de diminuir esses impactos ou prejuízos é muito dinâmica, pois varia em função dos ativos e dos riscos envolvidos.

Elaborar procedimentos para recuperação de desastres

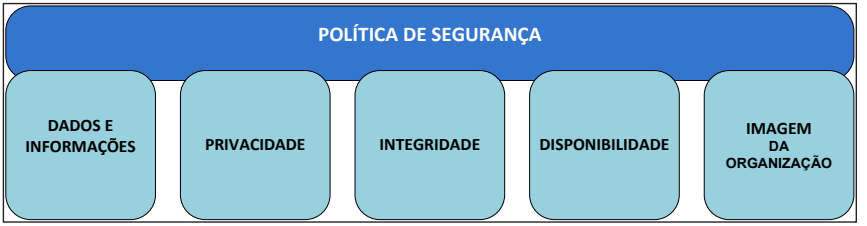
Caso um incidente de segurança ocorra, é necessário um plano para recuperação de desastre causado por essa ocorrência. Da mesma maneira que o objetivo anteriormente apresentado, os procedimentos para recuperação de desastres variam em função de ativos e riscos envolvidos.

A política de segurança é atribuída ao CSO (*Chief Security Officer*) em organizações de maior porte, pois, além das responsabilidades técnicas envolvidas, é necessário que essa política esteja alinhada ao planejamento estratégico. Assim, o CSO deve possuir habilidades para o desenvolvimento dessas atividades.

Em virtude de sua grande abrangência e complexidade, a política de segurança pode ser segmentada. A política de uso aceitável (*Acceptable Use Policy*), por exemplo, estabelece o padrão de comportamento aceitável para o uso dos recursos computacionais de uma organização, além de esclarecer os direitos e responsabilidades dos usuários. Essa política trata de um conjunto de regras aplicadas pelos gerentes ou administradores de rede. Neste estudo, abordaremos somente tais regras.

Para a elaboração de uma política de segurança, devemos ter definidos quais recursos serão protegidos e a quais ameaças estamos sujeitos, conforme mencionado anteriormente. Com base nessas especificações, a política pode demandar apenas algumas horas de trabalho e, consequentemente, um pequeno investimento. Em contrapartida, quanto mais complexa e abrangente a política de segurança, maior deverá ser seu orçamento.

Observe a Figura 4. Ela apresenta os principais recursos atingidos pela política de segurança.



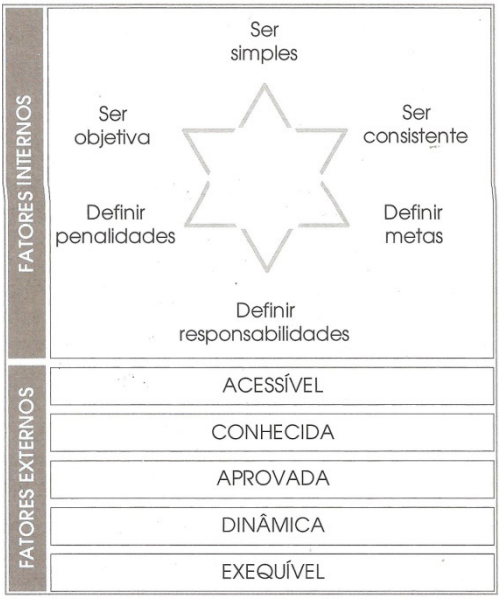
Fonte: adaptado de Campos (2007, p. 16).
Figura 4 *Principais recursos atingidos pela política de segurança*.

Ao analisar a Figura 4, é fundamental que você compreenda que esses recursos são variáveis de acordo com as políticas e os objetivos de cada organização e são sujeitos a ataques pela internet, tanto internos quanto externos.

Dando continuidade a essa explicação, observe que a política de segurança deve apresentar algumas características que garantam a sua aplicabilidade:

1) **Ser simples**: a política deve apresentar uma linguagem simples, facilitando sua leitura e compreensão.
2) **Ser objetiva**: a política não deve ser um documento muito extenso, deve apenas focar os objetivos a serem alcançados.
3) **Ser consistente**: a política deve estar alinhada com as demais normas, como, por exemplo, as legislações públicas.
4) **Definir metas**: a política deve apresentar as metas a serem alcançadas.
5) **Definir responsabilidades**: a política deve estabelecer as responsabilidades sobre o uso da informação.
6) **Definir penalidades**: a política deve conter procedimentos de punição caso não seja cumprida.

Observe, na Figura 5, as propriedades da política de segurança.



Fonte: Campos (2007, p. 142).
Figura 5 *Propriedades da política de segurança*.

Considerando ainda os fatores externos que envolvem a política de segurança, podemos citar suas características:

1) **Acessível**: a política deve ser acessível a todos.
2) **Conhecida**: seu conteúdo deve ser de conhecimento geral.
3) **Aprovada**: a política deve ser aprovada pela direção da organização, demonstrando aos demais colaboradores sua aceitação e seriedade.
4) **Dinâmica**: deve apresentar atualizações constantes.
5) **Exequível**: deve apresentar regras que possam ser praticadas.

Ainda tratando das características da política de segurança, ela deve conter diretrizes claras sobre os aspectos listados a seguir:

1) **Objetivo da segurança**: deve explicar de maneira simples e consistente os objetivos ou finalidades da política de segurança.

2) **A quem se destina**: deve identificar quais os departamentos e usuários aos quais a política se aplica.
3) **Propriedade dos recursos**: deve apresentar as regras para os vários aspectos relacionados com a propriedade de ativos de informações.
4) **Responsabilidades**: deve definir os tipos de responsabilidades relacionadas com o manuseio de ativos de informações.
5) **Requisitos de acesso**: deve indicar quais os requisitos a serem atendidos para o acesso aos ativos de informações.
6) **Responsabilização**: deve estabelecer punições para os casos de não cumprimento das regras.
7) **Generalidades**: deve incluir os aspectos não tratados nos demais aspectos.

Além das características apresentadas anteriormente, a política de segurança deve ser revisada e atualizada sempre que ocorrerem mudanças internas ou externas, tornando-se, desse modo, dinâmica. Por fim, é necessário que a política de segurança seja aprovada pela direção da organização, demonstrando aos demais colaboradores sua aceitação e seriedade.

A prática de uma política de segurança ainda é pouco difundida dentro das organizações, e, como todo e qualquer novo padrão, quando se pretende implementá-la, certamente encontraremos obstáculos. A fim de evitar ou minimizar essas resistências, o processo de implementação da segurança deve ser realizado em fases.

A primeira delas trata da mudança dos padrões culturais já estabelecidos na organização, iniciando as mudanças pelas demais áreas até atingir, por fim, as atividades dos sistemas informatizados.

Para que a política seja bem recebida, é preciso convencer as pessoas – ou a maioria delas – da sua importância para a empresa, isto é, deve-se vender a ideia, apresentando os benefícios da política de segurança de informações.

Antes, porém, da aplicação da política, é essencial o estabelecimento de uma política educacional em relação à segurança, divulgando-a por meio de palestras, *e-mail* informativo, apresentações, enfim, pelos meios de divulgação disponíveis na organização.

A seguir, apresentaremos um modelo sugestivo de política de segurança, lembrando que cada política deve ser elaborada para uso exclusivo, ou seja, atenderá as necessidades pontuais da organização para a qual foi criada.

Modelo de política de segurança

NOME OU LOGO DA EMPRESA XXX

Política de Uso do Acesso Corporativo à Internet

A informação contida neste documento é confidencial e de propriedade da Empresa XXX. Este documento não é para ser reproduzido ou distribuído fora da Empresa XXX.

1. OBJETIVO

Estabelecer regras para o uso apropriado da Internet na empresa XXX. O propósito da empresa em conceder o direito de acesso à Internet aos seus funcionários é, única e exclusivamente, permitir que os mesmos obtenham as informações necessárias ao desempenho das atividades corporativas de modo a atingir os objetivos de negócio da empresa.

2. ÂMBITO

Esta política abrange todos os funcionários autorizados a acessar a Internet através da rede corporativa da empresa XXX.

3. DEFINIÇÕES

Usuários – funcionários da Empresa XXX autorizados a acessar a Internet através da rede corporativa.

Internet – rede mundial de computadores.

Intranet – rede corporativa de computadores.

Acesso à Internet – inclui, mas não se limita, o acesso a web sites, o envio e recebimento de e-mails, a transmissão e o recebimento de arquivos e a execução de aplicativos de Internet, através de computadores da rede corporativa.

4. POLÍTICA

4.1 Uso Aceitável

O acesso à Internet concedido pelo escritório aos seus funcionários tem como objetivo ser utilizado como ferramenta para auxiliar os usuários na realização das tarefas corporativas diárias e a obter vantagens competitivas relacionadas aos negócios da empresa.

A Empresa XXX tem o direito de monitorar e controlar o acesso à Internet a partir da sua rede corporativa. Os usuários não devem ter qualquer expectativa de privacidade no que diz respeito à informação transmitida e/ou recebida através do(s) acesso(s) e recursos corporativos disponibilizados pela organização.

Devido à existência na Internet de pessoas e/ou organizações com intenções hostis, os usuários devem estar cientes da importância e da obrigatoriedade do correto uso dos requisitos de segurança disponíveis nos recursos corporativos que utilizam.

4.2 Uso Inaceitável

Os usuários não podem usar seus privilégios de acesso à Internet para:

- Envolver-se na observação ou na troca de materiais que tenham conteúdo de natureza odiosa, obscena, discriminatória, ofensiva ou visando assédio sexual;
- Envolver-se em qualquer tipo de negócios privados para obter lucros ou ganhos pessoais;
- Envolver-se em qualquer atividade ilegal, incluindo jogos de azar, carregar ou baixar softwares sem a permissão dos detentores de seus direitos de copyright e/ou softwares que estão sujeitos ao controle de exportação de seus países de origem;
- Interferir intencionalmente nas operações normais dos equipamentos da rede corporativa com a Internet (gateway de Internet), ou de qualquer outro site;
- Acessar materiais não relacionados aos negócios do escritório, tais como o acesso a rádios, a sites que distribuam imagens, áudio e/ou vídeo (streaming vídeo), diários eletrônicos (blogs) e etc.
- Baixar materiais não relacionados ao desempenho das atividades corporativas, como arquivos de imagens, áudio e vídeo e/ou programas de uso pessoal, mesmo que gratuitos (freewares);
- Tentar ganhar acesso não autorizado a outros serviços disponíveis na Internet;
- Enviar e/ou receber, mesmo que esporadicamente, e-mails excessivamente grandes ou mensagens de correntes eletrônicas;
- Envolver-se em atividades que violem políticas de outras empresas e/ou que possam ser contrárias aos interesses do escritório;
- Abrir ou baixar arquivos de sites da Internet, grupos de notícias (newsgroups), contas de e-mails externas ou de outras fontes, sem as devidas precauções para a detecção de vírus;
- Revelar informações confidenciais ou de propriedade da organização para destinatários não autorizados, através de qualquer meio;
- Transmitir informações confidenciais ou proprietárias para destinatários autorizados, localizados fora da rede corporativa, sem os devidos cuidados relativos à integridade das informações;
- Usar o aplicativo de mensagem instantânea corporativo (Messenger), para divulgar informações confidenciais ou de propriedade da organização para destinatários que não sejam usuários da rede corporativa;
- Divulgar contas, identificadores, senhas de acesso e/ou de usuário ou qualquer outro tipo de identificação corporativa pessoal, com pessoas ou programas localizados fora da rede corporativa.

5. SANÇÕES

Qualquer usuário que, comprovadamente, venha a violar a presente política corporativa estará sujeito, dependendo da gravidade da infração, a:

- Ter seu acesso à Internet restringido ou mesmo cancelado;
- Ter rescindido o seu contrato de trabalho ou de prestação de serviços;
- Responder a processo criminal.

6. CONTROLE DE VERSÃO

Versão: 01

Data: 24/04/2010

Autor: PAULO MORAES/Rio de Janeiro

Termo de Concordância das Condições de Uso dos Recursos Computacionais Corporativos

A informação contida neste documento é confidencial e de propriedade da Empresa XXX. Este documento não é para ser reproduzido ou distribuído fora da Empresa XXX.

Declaro ter lido o documento

Política de Uso do Acesso Corporativo à Internet de 03/04/2007, disponíveis na rede interna e impresso, e atesto que:

- Entendi e compreendi completamente o conteúdo das políticas;
- Estou plenamente ciente de que, em caso de violação das referidas políticas, estarei sujeito a ações disciplinares e legais.

Data: __/ __/ 20___

Nome: _____

Assinatura: _____

IMPORTANTE: Este documento deve ser anexado à pasta corporativa do funcionário (MORAES, 2011).

8. QUESTÕES AUTOAVALIATIVAS

Sugerimos que você procure responder, discutir e comentar as questões a seguir, que tratam da temática desenvolvida nesta unidade, ou seja, do valor agregado que uma política de segurança traz para as organizações e da análise de riscos às atualizações necessárias de tais políticas.

A autoavaliação pode ser uma ferramenta importante para você testar o seu desempenho. Se você encontrar dificuldades em responder a essas questões, procure revisar os conteúdos estudados para sanar as suas dúvidas. Esse é o momento ideal para você faça uma revisão desta unidade.

Lembre-se de que, na Educação a Distância, a construção do conhecimento ocorre de forma cooperativa e colaborativa; compartilhe, portanto, as suas descobertas com os seus colegas.

Confira, a seguir, as questões propostas para verificar o seu desempenho no estudo desta unidade:

1) Defina com suas palavras o significado do termo "acesso lógico".

2) Confidencialidade e integridade são características de segurança da informação. Detalhe com suas palavras a terceira característica, exemplificando-a.

3) Quais as contribuições trazidas pela Lei Sarbanes-Oxley?

4) O processo de implantação da segurança da informação não é uma tarefa simples. Você concorda com essa afirmação? Justifique sua resposta.

5) Explique por que os computadores (principalmente os conectados à internet) aumentam consideravelmente os riscos relacionados aos ambientes de informações.

6) Em sua opinião, por que funcionários demissionários devem ter seus acessos a recursos sensíveis bloqueados?

7) Cite os principais objetivos de uma política de segurança para a organização.

8) Qual é a importância da educação e conscientização de todos os colaboradores da empresa para a política de segurança?

9) Qual a primeira fase para elaboração de uma política de segurança?

10) Observando a Figura 4, explique com suas palavras cada um dos recursos atingidos por uma política de segurança.

11) A política de segurança elaborada para uma determinada organização pode ser aplicada a outra? Justifique sua opinião.

12) Você concorda com a afirmação de que somente os membros dos níveis de gerência e diretoria têm a obrigação de conhecer e cumprir as regras dispostas na política de segurança da organização? Justifique sua resposta.

13) Na ocorrência de um incidente de segurança da informação, qual dos impactos gera maiores prejuízos à organização: o desgaste da sua imagem ou as perdas financeiras? Justifique sua resposta.

14) Com base no modelo de política de segurança apresentado nesta unidade, elabore o esboço dos tópicos da política solicitada como parte dos estudos deste *Caderno de Referência de Conteúdo*.

15) Como a Lei Sarbanes-Oxley provoca impactos sobre empresas americanas no Brasil?

9. CONSIDERAÇÕES

Nesta unidade, foram abordados os conceitos relacionados à segurança de um sistema de informação, com ênfase na importância da implantação de uma política de segurança dentro das organizações.

Uma vez apresentados os fundamentos dos aspectos de segurança, na próxima unidade, trataremos das ameaças mais comuns a um sistema computacional, exemplificando como esses ataques ocorrem.

10. E-REFERÊNCIAS

Lista de figuras

Figura 3 *Resultado da 10ª Pesquisa Nacional de Segurança da Informação (2006)*. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>. Acesso em: 9 set. 2011.

Sites pesquisados

CERT.BR. *Cartilha de segurança para internet 3.1 (2006)*. Disponível em: <http://cartilha.cert.br/fraudes/sec1.html>. Acesso em: 25 maio 2011.

MÓDULO. *10ª Pesquisa Nacional de Segurança da Informação*. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>. Acesso em: 2 maio 2011.

MORAES, P. *PSI*: Política de Segurança da Informação. 2010. Disponível em: <http://segurancalinux.com/artigo/PSI-Politica-de-Seguranca-da-Informacao?pagina=3>. Acesso em: 24 jun. 2011.

11. REFERÊNCIAS BIBLIOGRÁFICAS

CAMPOS, A. L. N. *Sistema de segurança da informação*: controlando os riscos. 2. ed. Florianópolis: Visual Books, 2007.

CARUSO, C. A. A.; STEFFEN, F. D. *Segurança em informática e de informações*. 2. ed. rev. e ampl. São Paulo: Senac, 1999.

_____. _____. 3. ed. rev. e ampl. São Paulo: Senac, 2006.

COMER, D. E. *Redes de computadores e internet*. 4. ed. Porto Alegre: Bookman, 2007.

LAUDON, K. C.; LAUDON, J. P. *Sistema de informações gerenciais*. 7. ed. São Paulo: Pearson Prentice Hall, 2007.

EAD

Ameaças a um Sistema Computacional

2

1. OBJETIVOS

- Conhecer as principais técnicas utilizadas para comprometer um sistema.
- Conhecer e aplicar formas de inibir as principais ameaças a um sistema informatizado.

2. CONTEÚDOS

- IP *spoofing*.
- SYN *flood*.
- *Denial of Service*.
- Engenharia social.
- *Smurf*.
- Redes Wi-Fi.

3. ORIENTAÇÕES PARA O ESTUDO DA UNIDADE

Antes de iniciar o estudo desta unidade, é importante que você leia as orientações a seguir:

1) Nesta unidade, você estudará as principais técnicas utilizadas pelo *hacker* para invasão dos sistemas computacionais. Uma vez conhecidas as técnicas, o profissional de segurança deve buscar ferramentas de trabalho que garantam a estabilidade dos sistemas e, consequentemente, a segurança da informação.
2) Os conceitos a serem abordados podem ser assimilados mais facilmente a partir de debates, questionamentos e cooperação. Discuta os temas com seus colegas.
3) Para saber mais a respeito de ataque de SYN *flood*, um dos temas que será abordado nesta unidade, há informações detalhadas disponíveis no portal Security Focus: <http://www.securityfocus.com/advisories/211>. Acesso em: 2 set. 2011.
4) Sugerimos a leitura, na íntegra, de informações referentes ao conteúdo que será abordado no Tópico 6, *SYN flood*, no *site* disponível em: <http://www.symantec.com/connect/articles/hardening-tcpip-stack-syn-attacks>. Acesso em: 11 maio 2012.
5) Muitos sistemas de proteção foram desenvolvidos por especialistas de segurança em laboratórios complexos. Em contrapartida, algumas pessoas estudam tais sistemas a fim de verificar suas vulnerabilidades ou falhas. Elas são conhecidas como *hackers*. Alguns *hackers* se tornaram muito conhecidos por causa de ações que causaram grande impacto em redes de computação e telecomunicações. Antes de iniciar os estudos desta unidade, conheça um pouco da biografia dos principais *hackers* da atualidade.

Kevin Mitnick (1964-)

Kevin Mitnick começou suas atividades como *hacker* aos 17 anos, quando passou a fazer parte de um grupo *hacker* no seu colégio, em Los Angeles, já que possuía interesse em informática. Kevin invadiu, inicialmente, o computador da Monroe High School, onde estudava, para alterar as notas do curso.

Mais tarde, ingressou no *phreaking* (*hacker* de telefonia). Usando um computador e um *modem*, ele controlava centrais de várias empresas telefônicas. Obteve informações como manuais e programas de vários sistemas. Desse modo, sucederam-se invasões e roubos de informações sigilosas, que resultaram em sua prisão e obrigação de assistir palestras para seu vício por computadores. No entanto, após a soltura, suas ações continuaram, e Kevin tornou-se celebridade ao invadir o sistema do Comando de Defesa Aérea dos Estados Unidos. Ele foi preso dois anos mais tarde pelo FBI, acusado de causar prejuízo de mais de 80 milhões.

Ficou mais cinco anos preso e outros três em liberdade condicional. Hoje, Kevin é consultor em segurança de rede e autor de livros. No livro *A arte de enganar* (2003), apresenta alguns exemplos fictícios de invasão, utilizando a engenharia social, permitindo que o leitor entenda o raciocínio de quem o está atacando e alertando para o uso da persuasão e manipulação nos ataques, em conjunto com códigos e sistemas, o que resulta que a ação de um único funcionário possa comprometer o sistema de toda a organização.

No livro, Kevin Mitnick fornece, ainda, orientações para que se desenvolvam protocolos, programas de treinamentos e manuais que não ponham em risco a segurança adotada. Segundo Steve Wozniak, amigo de Kevin, que faz a apresentação do livro, ambos eram curiosos sobre o mundo e, como era próprio da idade, gostavam de testar novas coisas. Por meio do computador, podiam aprender, solucionar problemas e ganhar coisas. No entanto, as regras sociais não permitiam que eles explorassem livremente tudo aquilo que desejavam, apesar da emoção que aquilo lhes trazia, por permitir realizar coisas que outras pessoas acreditavam que não poderiam ser feitas. De acordo com Steve, apesar de Mitnick usar da engenharia social e a considerar ferramenta para trapacear pessoas, ele nunca a usou com o objetivo de enriquecer ou causar danos, mas, sim, pelo prazer por se sentir poderoso.

Kevin foi criado pela mãe, já que seu pai saiu de casa quando ele tinha apenas três anos de idade. Para sustentá-lo, sua mãe trabalhava muito, o que fez que ele cuidasse de si mesmo o dia todo. Aos 12 anos, descobriu como viajar de graça por Los Angeles, utilizando um bilhete de baldeação de ônibus, já que percebeu que os motoristas usavam um padrão de furos incomum para marcar o dia, a hora e o itinerário nos bilhetes, e foi orientado por um motorista amigo seu que ele poderia comprar aquele furador de papel especial. Ele obtinha passagens em branco nas lixeiras dos terminais, que eram descartadas pelos motoristas ao final dos turnos, e, assim, podia marcar suas próprias baldeações e viajar de ônibus para qualquer lugar de Los Angeles.

Mais tarde, ele descobriu seu interesse por mágica, e, ao aprender um novo truque, treinava-o até que saísse perfeito. Foi assim que ele descobriu o seu prazer em enganar pessoas.

No ginásio, Kevin tornou-se amigo de outro aluno que praticava *phone phreaking*, que o mostrou como poderia usar um telefone para obter informações que a empresa telefônica tinha sobre um cliente e como usar números de teste secretos para fazer ligações interurbanas sem pagar. Kevin ouvia as ligações das empresas de telefonia e ia aprendendo sobre o linguajar e os procedimentos utilizados pelos funcionários. Aos 17 anos, Kevin já conhecia tudo sobre as centrais telefônicas, não apenas a eletrônica, as centrais e os computadores, mas sobre procedimentos e terminologias.

No colégio, ele foi aceito por um grupo de pessoas que passava boa parte de seu tempo desenvolvendo programas mais eficientes que não tivessem etapas desnecessárias e pudessem fazer um trabalho mais rápido. Quando concluiu os estudos, fez um curso de computadores no Computer Learning Center, em Los Angeles, e, em alguns meses, percebeu a vulnerabilidade no sistema operacional e ganhou privilégios administrativos no uso do seu microcomputador, o que foi percebido pelo gerente da escola. Os especialistas do corpo docente não conseguiram descobrir como ele havia feito aquilo, e ele recebeu a proposta de criar um projeto para melhorar a segurança dos computadores da escola.

Kevin considerava-se com o perfil para ser um engenheiro social, que, segundo ele, tem inclinações para enganar pessoas, com talentos de influenciar e persuadir. Mas, segundo ele, o engenheiro social usa essas habilidades não para trapacear as pessoas ou ganhar dinheiro, mas, sim, contra as empresas, para obter suas informações. Kevin considerava-se, ainda, com um talento para descobrir segredos que ele não deveria saber, assim, convencia, por exemplo, alguém do outro lado do telefone a lhe fornecer informações sigilosas, utilizando pretextos com o intuito de aprimorar sua habilidade.

Kevin teve acesso não autorizado a sistemas de computadores de grandes corporações que eram altamente protegidos, usando meios técnicos e não técnicos. Obteve, assim, o código-fonte de sistemas operacionais e dispositivos de telecomunicações para estudar vulnerabilidades e o funcionamento interno deles. O motivo dessas ações era sua própria curiosidade intelectual, e, dessa forma, ele podia descobrir informações de tudo aquilo que despertasse o seu interesse. Tinha interesse em saber tudo sobre o funcionamento da rede de telefonia e as falhas na segurança dos computadores.

Hoje, segundo ele, não é mais motivado apenas pela curiosidade; reuniu seu extenso conhecimento sobre segurança e engenharia social para ajudar o governo, as empresas e os indivíduos a evitarem ameaças à segurança da informação. Realiza consultorias, *workshops*, e já teve um programa no rádio, alertando para possíveis vulnerabilidades dos sistemas de informação (imagem disponível em: <http://mitnicksecurity.com/speaking.php>. Acesso em: 28 jul. 2011. Texto adaptado do *site* disponível em: <http://mitnicksecurity.com/media/Kevin_Mitnick_Bio_BW.pdf>. Acesso em: 28 jul. 2011).

Kevin Poulsen

Kevin Poulsen ganhou notoriedade em 1982, quando a procuradoria de Los Angeles o acusou de ter obtido acesso não autorizado a uma dúzia de computadores da ARPANET, a precursora da Internet. Naquela época Poulsen tinha apenas dezessete anos, e não foi indiciado. Ele foi trabalhar como programador e supervisor de segurança na SRI Internacional na Califórnia e depois como administrador de rede na Sun Microsystem. Em 1987, agentes de segurança da Pacific Bell

descobriram que o *hacker* e seus amigos estavam invadindo os prédios e os computadores da companhia de telefone. Depois de descobrir que Poulsen também trabalhava para um contratador de defesa, o FBI começou um processo de espionagem contra ele. Diante da possibilidade de ser detido sem direito a fiança, Poulsen se tornou um fugitivo. Durante a fuga, ele obteve informações sobre os métodos de investigação eletrônica do FBI, além de invadir os computadores da Bell Computers para trapacear em um concurso por telefone de uma estação de rádio e ganhar um Porche 944-S2 e férias no Havaí. Poulsen finalmente foi capturado no dia 10 de abril de 1991 por um agente de segurança da Pacific Bell que recebeu pistas de um informante. No dia 4 de dezembro de 1992, ele se tornou o primeiro *hacker* a ser indiciado sob as leis americanas de espionagem quando o departamento de justiça o acusou de roubar informações sigilosas. Poulsen foi preso sem direito a fiança e lutou contra as acusações de espionagem até que foram retiradas. Poulsen ficou preso durante cinco anos e dois meses até que foi solto em 4 de junho de 1996, quando ele começou um período de três anos de liberdade supervisionada, no qual ficou o primeiro ano proibido de possuir um computador e o ano e meio seguinte proibido de acessar a Internet (imagem disponível em: <http://www.hasnul.net/news.php?default.0.20>. Acesso em: 17 set. 2010. Texto disponível em: <http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=30>. Acesso em: 17 set. 2010.).

Robert Tappan Morris

Há 20 anos, às 18h do dia 2 de novembro de 1988, Robert Tappan Morris, estudante da Universidade Cornell, estava no MIT (Instituto Tecnológico de Massachusetts) distribuindo o que seria considerado o primeiro código malicioso a se espalhar pela internet. O "Morris *worm*", como ficou conhecido, alastrou-se rapidamente e inutilizou muitos sistemas que contaminou. Estimativas sugerem que a praga infectou 10% dos 60 mil computadores que formavam a rede mundial da época.

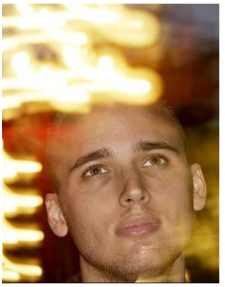
O "*worm"* pegou de surpresa os administradores e usuários da internet naquele ano, que nunca tinham visto um ataque parecido. Embora o vírus não tivesse nenhuma carga maliciosa, um problema em sua programação sobrecarregava alguns sistemas infectados, impedindo sua operação.

Para se espalhar, a praga tirava proveito de brechas de segurança existentes em softwares como o sendmail – responsável pelo envio de correio eletrônico – e o fingerd – um fornecedor de informações de usuários. Apenas computadores com BSD 4 e Sun 3, ambos baseados em Unix, eram infectados. Quase todos os *worms* semelhantes que apareceram desde então atacaram sistemas Microsoft: Blaster, Slammer, Code Red e Sasser. O último grande ataque do gênero contra sistemas Unix foi o Slapper, em 2002.

Além de dar início à valorização da segurança em softwares, a mais notável consequência do episódio foi a criação do CERT (http://www.cert.org), um time de especialistas responsável pela comunicação e tratamento de incidentes de segurança. Muitos países e mesmo empresas hoje possuem equipes com o mesmo objetivo. Quem realiza estas funções na rede brasileira é o CERT.br (http://www.cert.br).

Robert Tappan Morris, criador da praga, foi condenado por fraude em computadores em 1990. Não foi para a cadeia, mas teve que pagar uma multa de US$10 mil dólares e prestar 400 horas de serviços comunitários. Quando Robert disseminou o vírus, seu pai, Robert Morris, trabalhava na Agência Nacional de Segurança dos EUA. Hoje, o "criador do primeiro vírus" é professor no MIT – a mesma instituição em que ele iniciou a propagação de seu *worm* (imagem e texto disponíveis em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL846193-6174,00-PRIMEIRO+VIRUS+DISSEMINADO+PELA+INTERNET+COMPLETA+ANOS.html>. Acesso em: 3 maio 2011).

Adrian Lamo



Adrian Lamo, 29 anos, se tornou o mais famoso "*hacker* do chapéu cinza" da década passada. Em 2003, invadiu o sistema do jornal The New York Times apenas para incluir a si mesmo na lista de colaboradores. O jornal não achou graça na brincadeira e denunciou Lamo ao FBI. Em 2004, ele se declarou culpado da invasão e de também ter acessado os sistemas do Yahoo, Microsoft e WorldCom, recebendo sentença de seis meses de prisão domiciliar na casa dos pais e mais dois anos de liberdade vigiada.

Seis anos depois, ele se tornou, em junho, um renegado na comunidade *hacker*. No último dia 8 veio a público que Lamo denunciou ao FBI o soldado Bradley Manning, 22 anos, analista de inteligência do exército americano, como o responsável pelo vazamento de informações confidenciais sobre a Guerra do Iraque, inclusive do polêmico vídeo, divulgado em abril, em que um helicóptero Apache dispara contra civis. Manning, que aparentemente agiu contra a guerra, procurou Lamo após a publicação, em abril, pela revista Wired, de que o ex-*hacker* é portador da Síndrome de Asperger, uma forma de autismo, em busca de apoio. Considerava os dois "almas irmãs", mas Lamo não pensou assim, alegando que com a denúncia salvaria vidas de militares americanos em combate.

Caiu, a partir de então, em desgraça com os ex-fãs. O site sueco Wikileaks, que publica informação confidencial de governos e empresas e pôs na internet o vídeo do ataque de helicóptero, chamou-o de "notório ladrão de informação e manipulador".

Lamo, hoje um consultor de segurança de empresas, também vive a situação inusitada de ser cumprimentado, graças a seu "patriotismo", por pessoas que antes o criticavam pela vida de *hacker* (imagem e texto adaptado disponíveis em: <http://www.terra.com.br/noticias/tecnologia/infograficos/hackers/hackers-01.htm>. Acesso em: 3 maio 2011).

4. INTRODUÇÃO À UNIDADE

Na unidade anterior, você teve a oportunidade de compreender os conceitos de segurança de um sistema, bem como a necessidade de coleta adequada das informações para melhor análise de riscos e definição de política de segurança adequada.

Considerando os conteúdos estudados anteriormente, iniciaremos esta unidade conhecendo as principais ameaças a um sistema computacional, a fim de entendermos como elas são originadas.

Portanto, é fundamental que você compreenda que, atualmente, todos os sistemas de uma empresa são interconectados, o que proporciona agilidade nos processos, compartilhamento das informações e acesso móvel. Entretanto, essa mesma infraestrutura, utilizada para disponibilizar tais facilidades, pode fornecer acessos indevidos a pessoas não autorizadas, comprometendo a segurança e a integridade das informações pertinentes.

A partir do momento em que conhecemos melhor as vulnerabilidades de um sistema, podemos adotar medidas para contornar ou mesmo anular essas ameaças.

De acordo com Caruso (1999), podemos classificar os tipos de ataques em três grandes categorias: acesso não autorizado, impedimento de uso do equipamento e roubo de informações.

- **Acesso não autorizado**: é o tipo mais comum de ataque, no qual os atacantes obtêm acesso aos equipamentos. Pode ser evitado por meio do uso de identificação e requerimento de senhas de autenticação.
- **Impedimento de uso do equipamento**: o atacante faz que seu equipamento execute determinados serviços, tornando-o tão ocupado que você não tenha acesso a ele.
- **Roubo de informações**: é considerado o mais lucrativo dos tipos de ataque. Os atacantes buscam primeiramente capturar as senhas de acesso para posteriormente tomar posse de informações confidenciais.

Da mesma maneira que existem vários tipos de ataques, os motivadores que levam os atacantes a realizá-los também se diferenciam. Apresentaremos, a seguir, os quatro principais grupos de tipos de atacantes.

1) **Competição**: são motivados pelo espírito de competição dentro do grupo, ou seja, são classificados de acordo com a quantidade e complexidade de ataques bem-sucedidos.
2) **Divertimento**: buscam somente investigar os sistemas alheios em busca de dados que julgam interessantes e normalmente não são mal-intencionados.
3) **Espionagem**: visam o lucro, ou seja, após tomarem posse de informações importantes, tentam convertê-las em dinheiro.
4) **Vandalismo**: agem simplesmente pelo prazer de destruir, ou seja, atacam *sites* que consideram estar em desacordo com suas opiniões.

Mesmo diante de todo o esforço desprendido na tentativa de garantir a segurança da informação – alvo de ataques e acessos não autorizados –, uma grande parcela dos incidentes de segurança está relacionada a usuários devidamente autorizados que não seguem uma política de segurança ou mesmo estão mal treinados.

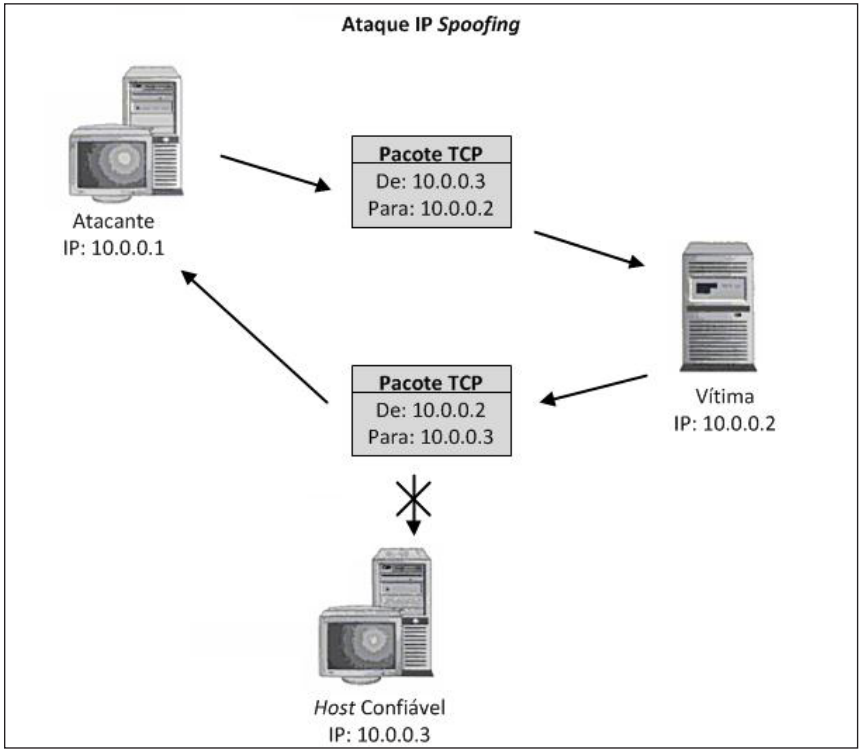
5. IP SPOOFING

A técnica de IP *spoofing* (mascarar) é amplamente difundida em redes locais e consiste em alterar os pacotes IP de saída, fazendo que um endereço de remetente falso seja enviado a toda a rede.

Observe que o encaminhamento de pacotes com endereços de remetentes falsos é possível em virtude da falta de mecanismos de controle do remetente do protocolo IP, fazendo que o pacote seja encaminhado ao destinatário sem nenhuma verificação ou validação do remetente.

Essa característica do protocolo IP torna a técnica de IP *spoofing* algo relativamente simples, pois tudo que o atacante necessita é manipular seu endereço lógico, e todos os ativos de rede encaminharão seus pacotes com destinatários falsos.

Veja, na Figura 1, como ocorre esse processo.



Fonte: adaptado de Maiwald (2003, p. 66).
Figura 1 *Encaminhamento de pacote em um ataque IP spoofing*.

Na Figura 1, observamos a vítima recebendo um pacote com endereço de origem falso.

Veja que a estação da vítima reconhece a relação com o *host* confiável e libera acesso a recursos solicitados por esse *host*. Aproveitando-se dessa situação, o atacante utiliza aplicações capazes de alterar seu endereçamento, passando a usar o mesmo endereçamento do *host* confiável para transmissão. Com isso, a estação da vítima não vai diferenciar as solicitações vindas do *host* confiável e do atacante, pois ambas possuem o mesmo endereço de destinatário.

Quando se utiliza IP *spoofing* para forjar um endereço de alguma outra estação da rede, cria-se uma forma de monitorar as

sessões em andamento, pois todo o tráfego, que inicialmente seria encaminhado apenas para a estação real, também passa a ser para a estação falsa.

Com a ajuda de um *sniffer* (canalizador de protocolos), é possível analisar e remontar todos os pacotes destinados inicialmente à estação real, o que permite que as sessões em andamento sejam monitoradas sem que o usuário perceba, pois sua estação continuará a receber todas as requisições que por ela foi solicitada.

Muitas políticas de segurança são baseadas em autenticações em endereços IPs. Uma vez que uma determinada estação tem a capacidade de alterar seus pacotes de saída, fazendo-se passar por outra estação com maior nível de confiabilidade, o atacante passa a ter um mesmo nível de confiabilidade, facilitando, assim, o acesso a outras estações ou servidores.

A forma mais eficiente de se inibir esse tipo de ataque é filtrá-lo no roteador, bloqueando pacotes que entram na rede com endereço de origem local.

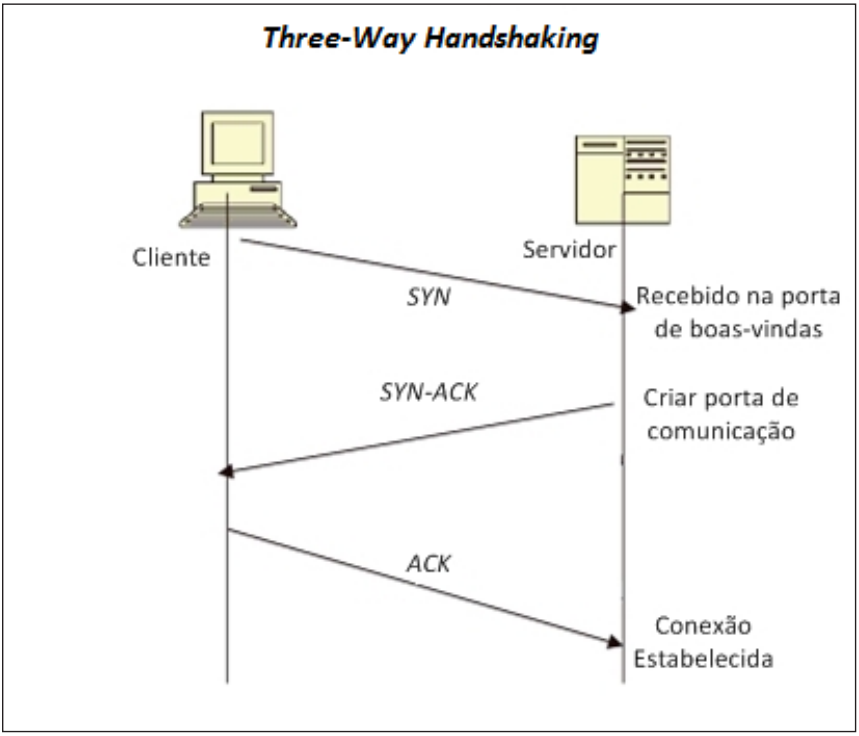
Essa forma de ataque ficou muito conhecida por ter sido utilizada pelo famoso *hacker* Kevin Mitnick, como foi mencionado em sua biografia, no Tópico 3, ao invadir a rede particular de Tsutomu Shimomura, um dos maiores especialistas em segurança dos Estados Unidos.

6. SYN FLOOD

O ataque SYN *flood*, também conhecido como "ataque SYN", tem como objetivo consumir os recursos de um determinado servidor, provocando um *Denial of Service* (DoS) e causando lentidão ou interrupções de conexão. Essa forma de ataque utiliza o mecanismo de inicialização de sessão do protocolo TCP. Esse mecanismo é chamado de *three-way handshaking*.

No processo de inicialização de sessão do protocolo TCP, **são enviadas três mensagens:** SYN, SYN/ACK e ACK.

Veja, na Figura 2, o mecanismo de inicialização.



Fonte: adaptado de Kizza (2008, p. 135).
Figura 2 *Abertura de sessão* no protocolo *TCP (three-way handshaking)*.

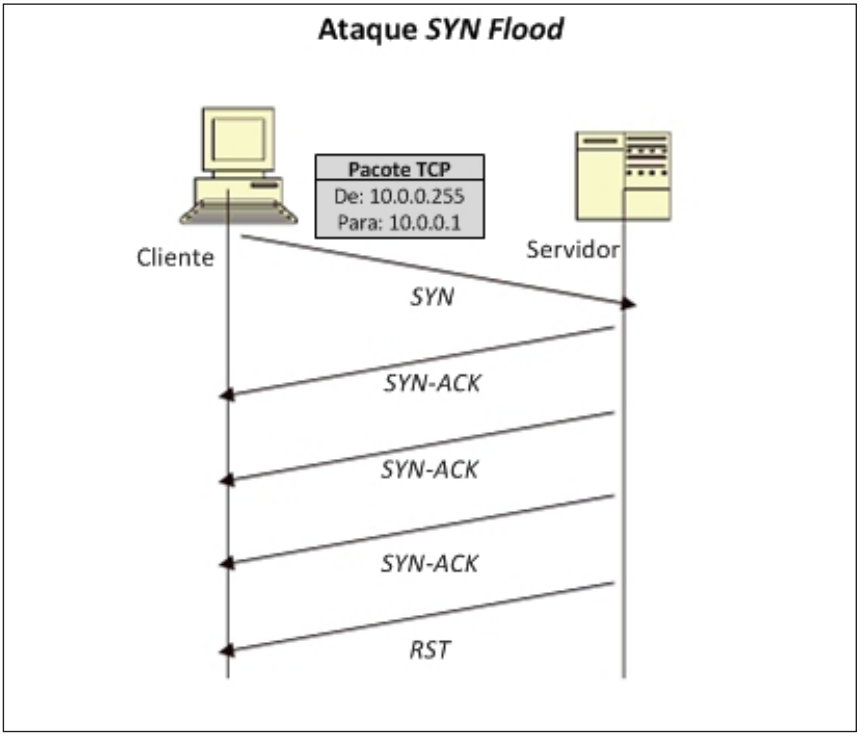
Na Figura 2, podemos observar o momento em que se inicia a sessão. Após essa etapa, os demais pacotes são enviados pelo cliente ao servidor.

Em um ataque SYN *flood*, são enviadas várias mensagens SYN ao servidor, contendo endereço de destino falso. Ao receber uma mensagem SYN, o servidor envia como resposta a mensagem SYN+ACK, porém, como não obtém nenhuma resposta, o servidor torna a enviar essa mensagem várias vezes.

Cada mensagem SYN+ACK enviada pelo servidor na tentativa de responder a esse ataque será enviada como *broadcast* na rede.

Isso acontece porque normalmente o ataque SYN *flood* é realizado utilizando, também, a técnica de IP *spoofing*. Por fim, a conexão é encerrada por meio do envio da mensagem RST (*reset*).

Veja, na Figura 3, um esquema dessa troca de mensagens.



Fonte: adaptado de Kizza (2008, p. 135).
Figura 3 *Resposta de um servidor a um ataque SYN flood*.

Na Figura 3, constatamos as tentativas do servidor em responder a uma requisição encaminhada com endereço de origem falso, um endereço de *broadcast*.

Segundo informações adaptadas da *home page* da Symantec (2012), os ataques de SYN *flood* já deixaram alguns provedores de acesso em estado de colapso, obrigando-os, assim, à implementação de proteções na pilha TCP/IP, destacando-se a proteção conhecida como *syn cookies*.

Por meio dos SYN *cookies*, o servidor retarda a alocação de recursos uma vez recebido o datagrama sinalizado para sincronização SYN. O detalhamento desse mecanismo é apresentado a seguir:

1) O número de sequência inicial (NSI) é devidamente alterado ao invés de ser gerado aleatoriamente.
2) As informações que seriam armazenadas na tabela de estado são utilizadas pelo servidor para criação do NSI logo após o recebimento do primeiro datagrama SYN.
3) O número criado é adicionado ao datagrama SYN+ACK de retorno ao cliente.
4) O terceiro datagrama ACK, enviado pelo cliente, chega ao servidor com o valor de sequência acrescido de 1, sendo assim, NSI+1, que reserva recursos para a conexão depois do encerramento do *three-way handshake*.

Nos sistemas Linux, esse controle ou mecanismo de segurança é iniciado da seguinte forma: echo 1 > /proc/sys/net/ipv4/tcp_syncookies.

Se de maneira simples o controle é implementado em ambientes Linux, em plataformas baseadas nos sistemas operacionais Microsoft Windows 2000 e 2003, os procedimentos tornam-se mais complexos e se apresentam no registro:

- Nas entradas de registro localizadas em *HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters*, a entrada *SynAttackProtec* (*DWORD*), pode aceitar valores de 1 ou 2, alterado conforme a interpretação de um ataque de SYN *flood*.
- O controle de segurança é carregado por meio da análise das conexões TCP com valores existentes nas entradas do registro TcpMaxHalfOpen, TcpMaxHalfOpenRetried e TcpMaxPortsExhausted.

7. DENIAL OF SERVICE

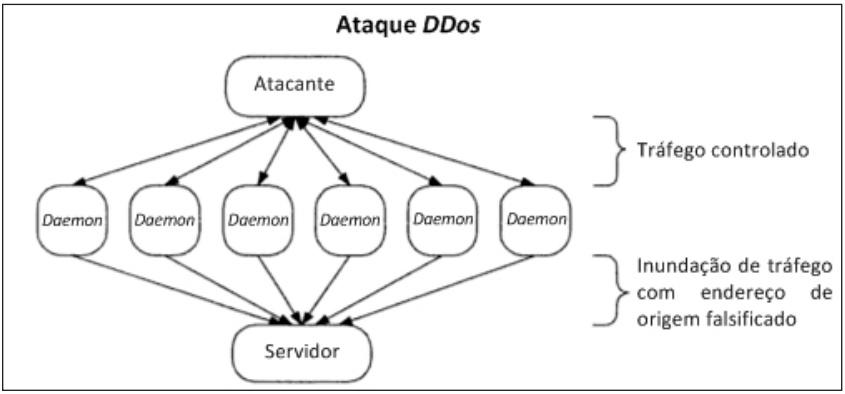
Denial of Service (DoS), ou negação de serviço, é uma forma de ataque com o objetivo de provocar a interrupção de serviços e recursos da vítima, causando a indisponibilidade do acesso das estações àquele determinado servidor. Essa forma de ataque é realizada sem que haja a necessidade de se conseguir acesso à vítima.

Vale ressaltar que todos os recursos de um servidor são limitados (memória, CPU, interface de rede, entre outros). Para atender às solicitações de clientes, os servidores precisam alocar parte desses recursos.

Com base nisso, um ataque de DoS só precisa enviar um alto número de requisições a um servidor, explorando alguma falha nos sistemas. Quando os recursos são consumidos, os serviços providos deixam de responder adequadamente às requisições dos clientes legítimos.

Existem duas formas de se fazer um ataque de DoS:

1) **Ataque direto**: o atacante envia requisições diretamente ao servidor, explorando alguma vulnerabilidade do sistema. Essa forma de ataque é limitada, pois uma estação dificilmente consegue consumir todos os recursos de um servidor.
2) ***Distributed Denial of Service* (DDoS)**: essa forma de ataque é mais complexa e envolve diversas outras estações, sendo enviadas requisições simultaneamente a um determinado servidor, e a quantidade de requisições pode ser extremamente maior. Assim, em um intervalo de tempo muito menor, é possível consumir todos os recursos disponíveis em um servidor.



Fonte: adaptado de Marshall (2001, p. 6).
Figura 4 *Ataque DDoS*.

Na Figura 4, apresentamos a forma de acionamento de um ataque de DDoS. Observe que, para se criar um ataque DDoS, o atacante necessita de muito planejamento. Além disso, precisa assumir o controle de várias estações que, para tal, normalmente utilizam algum *worm* (programa similar a vírus que se propaga automaticamente) para infectar essas estações.

Esses *worms* são programados para manter portas de comunicações abertas, pelas quais o atacante envia comandos às máquinas infectadas, mantendo-as sob seu controle. Essas estações infectadas são conhecidas como *daemons* (zumbis).

Quando se tem uma quantidade considerável de *daemons*, o atacante envia um comando solicitando que todos iniciem diversas requisições a servidores, o que causa sobrecargas sobre o *link* e, principalmente, sobre a memória. Para fazer as requisições desse tipo de ataque, em geral, é utilizado o protocolo TCP.

Esse protocolo trabalha com conexão de sessão, e são criadas várias sessões que permanecem abertas por um determinado período, mesmo que inativas, consumindo os recursos de um servidor.

Os primeiros registros percebidos pelo ataque de DoS são de 1998. Observe, na Tabela 1, a lista dos principais aplicativos para ataques de DoS e DDoS.

Tabela 1 Aplicativos de DoS e DDoS.

APLICATIVOS UTILIZADOS EM ATAQUES DoS E DDoS		
Fapi	TFN	TFN2K
Blitznet	Stacheldraht	Trank
Trin00	Shaft	

Não existe uma forma totalmente eficiente de se evitar um ataque DoS; entretanto, algumas ações, como as listadas a seguir, diminuem os riscos desse ataque.

1) **Aumentar a segurança do *host***: a principal forma de ataque de negação de serviço (DoS) é a distribuída. Assim, torna-se fundamental ter um alto nível de segurança nos *hosts*, para que estes não sejam utilizados como *daemons*.
2) **Atualização do sistema**: manter os sistemas operacionais e aplicações atualizados é de fundamental importância, pois vulnerabilidades conhecidas podem ser corrigidas com a instalação dos *patchs* e atualizações.
3) **Limitar largura de banda**: roteadores mais avançados possuem formas de limitar a largura de banda por tipos de pacotes em um ataque DDoS, que se caracterizam por gerar um tráfego muito grande de pacotes ICMP (*Internet Control Message Protocol*) e TCP SYN. Assim, regras são criadas e implementadas no roteador, limitando a largura de banda para tais pacotes.
4) **Planos de contingência**: todo sistema interligado à internet é passivo de algum tipo de ataque não previsto. Dessa forma, é necessário o emprego de planos de contingências em caso de falha dos serviços.

8. ENGENHARIA SOCIAL

Todas as tecnologias de proteção se tornaram cada vez mais eficientes ao longo do tempo. Ações como proteções individuais aos *hosts*, filtros mais minuciosos nos perímetros da rede e antivírus mais avançados tornaram o ambiente menos vulnerável às tentativas de acesso de atacantes. Todas essas proteções fizeram

que uma técnica antiga fosse aprimorada nos tempos atuais, com o objetivo de se coletar informações das vítimas utilizando recursos de persuasão. É a chamada **engenharia social**.

O processo de evolução de todos os sistemas é o responsável pela segurança de um ambiente e nos mostrou que, atualmente, o elo mais fraco dessa corrente é o homem.

A técnica de engenharia social não visa acessar às informações de maneira tradicional. As armadilhas são montadas com o objetivo de induzir os usuários a fornecerem deliberadamente informações que, em um primeiro momento, não parecem ser importantes, mas, quando são reunidas todas as informações obtidas nesse processo, pode-se observar o quão eficiente é essa forma de ataque.

Pessoas que se dispõem a utilizar essa técnica normalmente têm grande capacidade de se comunicar e de influenciar suas vítimas. Utilizam muitas informações coletadas do ambiente da vítima e são capazes de induzi-la a fornecer informações importantes involuntariamente.

A engenharia social pode ser percebida nos *sites* de relacionamento, os quais estão em grande expansão por todo o mundo, seja no âmbito pessoal, seja no profissional. A cada dia, torna-se mais comum o uso desse tipo de ferramenta dentro de uma corporação, aproximando, assim, clientes, fornecedores e parceiros. Entretanto, isso também proporciona um aumento significativo nas informações importantes disponíveis na internet, ao alcance de qualquer pessoa. A vulnerabilidade dessas informações contribui para o desenvolvimento de ataques cada vez mais sofisticados.

Na internet, a técnica de engenharia social é utilizada principalmente na forma de *phishing*, utilizando-se dos mais comuns meios de comunicação. Veja, a seguir, como isso pode ocorrer na prática e por meio de quais ferramentas.

1) ***E-mail***: utiliza-se de *e-mails* com conteúdo fraudulento com o objetivo de coletar informações pessoais, como

senhas e número de cartão de crédito. Um golpe muito comum que podemos citar são *e-mails* enviados como se fossem de um banco solicitando atualização cadastral de um cliente.

2) ***Sites***: *sites* falsos são construídos com o objetivo de coletar as informações que forem digitadas. Esses *sites* normalmente são idênticos aos originais, tornando difícil para o usuário distinguir o falso do autêntico.
3) **Mensagens instantâneas**: o ambiente mais descontraído é o ideal para os golpistas agirem, utilizando-se de programas conhecidos, como *malwares* (programas com o objetivo de se infiltrar em um computador e coletar informações). O golpista envia mensagens aos contatos da lista, na qual supostamente há uma foto ou algum outro tipo de anexo, e, ao acessar o *link*, o *malware* é instalado.
4) **Comunidades de relacionamento**: usam a mesma técnica utilizada nos ataques a aplicativos de mensagens instantâneas aplicadas a comunidades de relacionamento, também provocando o envio de mensagens aos contatos da lista que contém o *link* para a instalação de um *malware*.

Para se proteger de fraudes originadas de engenharia social, deve-se:

- investir em treinamento para os usuários, a fim de alertá-los acerca desses tipos de armadilhas e preveni-los;
- limitar os acessos externos apenas ao que é de escopo da corporação;
- utilizar sistemas de prevenções de intrusões (IPS), que, na verdade, são ferramentas instaladas em alguns pontos da rede que monitoram continuamente o tráfego, detectando e bloqueando ataques dessa natureza.

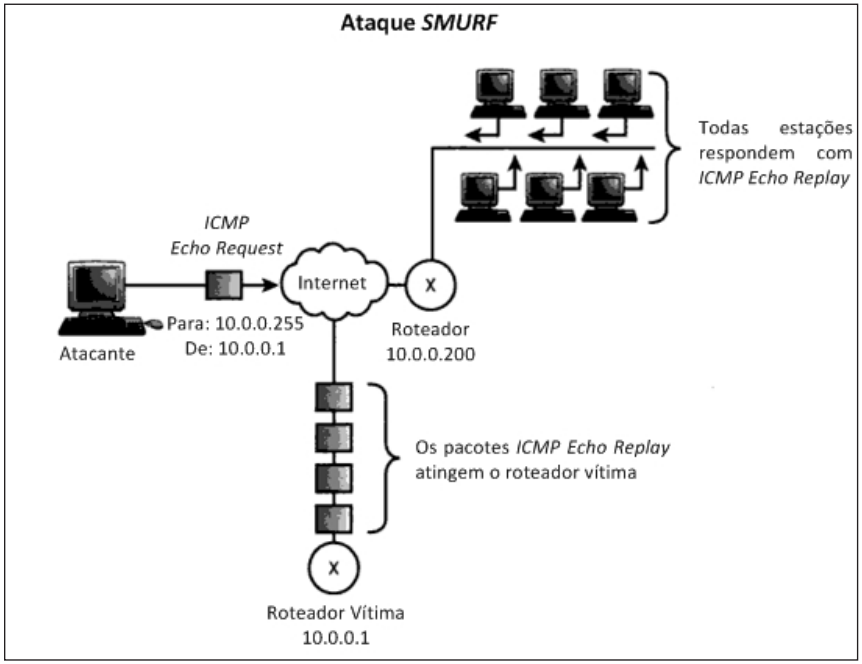
9. SMURF

O *smurf*, também conhecido como "ataque por reflexão", é uma forma de ataque bastante simples, que tem como objetivo causar um DoS em seu alvo ao utilizar pacotes ICMP.

Em uma rede TCP/IP, constantemente existe a necessidade de alguma estação, servidor ou equipamento de rede enviar pacotes a todos os *hosts* conectados à rede. Para isso, são utilizados os endereçamentos de *broadcast*. Cada pacote destinado a um endereço de *brodcast* será encaminhado a toda a rede.

O ataque *smurf* utiliza-se desse mecanismo de comunicação para induzir as estações pertencentes a um determinado domínio de *broadcast* a enviar respostas a uma requisição de ICMP com o endereço de origem falsificado.

A Figura 5 apresenta a forma como um ataque *smurf* acontece.



Fonte: adaptado de Burnett et al. (2001, p. 362).

Figura 5 *Encaminhamento de pacotes em um ataque smurf*.

Na Figura 5, observamos um ataque *smurf*, no qual podemos visualizar um pacote ICMP (*ping*). Essa requisição (*ping*) teve seu endereço de origem alterado para o da vítima (utilizando técnicas

como IP *spoofing*). Assim, a requisição *ping* é encaminhada a um endereço de *broadcast*, e isso faz que todas as estações ligadas à rede recebam essa requisição ICMP e enviem uma resposta ao endereço da vítima, sobrecarregando, desse modo, os recursos disponíveis.

Também é possível fazer um ataque *smurf* utilizando o protocolo UDP, porque todos os pacotes encaminhados à Porta 7 são retransmitidos de volta à origem, exatamente igual ao ICMP.

Uma forma bastante efetiva de se prevenir de um ataque *smurf* é filtrar os pacotes ICMP (*ping*) para endereços de *broadcast*.

Outra técnica que deve ser empregada para se evitar ataques *smurfs* é implementar segmentações na rede sempre que possível, diminuindo, então, as possíveis áreas de impacto de um ataque como esse.

10. REDES WI-FI

Atualmente, a utilização das redes Wi-Fi cresce de maneira considerável, o que proporciona uma gama bastante variada de aplicações, permitindo que localidades sejam cobertas, nas quais as redes cabeadas enfrentariam sérios problemas.

Entretanto, toda essa facilidade também pode se tornar um ponto vulnerável em um sistema computacional, pois, diferentemente da rede cabeada, as redes Wi-Fi muitas vezes não se restringem aos muros de uma corporação. Locais públicos, por exemplo, que possuem as redes Wi-Fi se tornaram os principais alvos de ataques. Aeroportos e *shoppings* também proporcionam um fácil acesso para circulação de pessoas, facilitando esses ataques.

Por seu tráfego não estar restrito como o de uma rede cabeada, as redes Wi-Fi tiveram que desenvolver uma camada a mais de proteção para que a sua utilização fosse segura e viável. Entretanto, ao longo do tempo, muitas dessas tecnologias desenvolvidas para proteção de rede Wi-Fi foram sendo burladas com aplicações de sonda bastante sofisticadas.

Protocolos WEP e WPA

Inicialmente, o principal meio de proteção de uma rede Wi-Fi foi o protocolo de WEP (*Wired Equivalent Privacy*), que criptografava os dados que são enviados pelo sinal Wi-Fi. No entanto, logo foram desenvolvidas aplicações capazes de coletar os dados criptografados e extrair a chave criptográfica, permitindo, assim, o acesso a redes criptografadas com WEP.

Para substituir esse protocolo, foi desenvolvido outro, de criptografia, denominado WPA (*Wi-Fi Protected Access*). Esse protocolo pode ser utilizado com uma chave temporária (TKIP). Entretanto, em 2009, pesquisadores das universidades Hiroshima e Kobe, no Japão, desenvolveram um sistema capaz de quebrar a criptografia WPA com TKIP, até então considerada segura.

Atualmente, existe uma grande variedade de aplicativos capazes de quebrar criptografias Wi-Fi, tais como *wepcrack*, WPA *crack* e *backtrack*. Basicamente, esses aplicativos funcionam coletando informações criptografadas que são transmitidas pela rede Wi-Fi. Após o período de coleta, esses dados são utilizados para aplicação de algoritmos capazes de revelar a chave de criptografia utilizada e, com isso, obter acesso à rede Wi-Fi.

Access Point Spoofing

O ataque *Access Point Spoofing* (associação maliciosa) é um dos principais ataques a redes Wi-Fi. Para que ocorra, é disponibilizada uma rede Wi-Fi falsa dentro da mesma área de cobertura da autêntica, fazendo que as vítimas que se conectam não percebam que não estão conectadas à rede Wi-Fi autêntica. Para isso, o atacante necessita de um *software* que simula um *access point* (ponto de acesso a partir da sua conexão Wi-Fi).

O *HostAp* é um exemplo de *software* com essa função. Normalmente, essa técnica é utilizada após o atacante obter conexão na rede Wi-Fi autêntica. Com isso, é possível redirecionar o tráfego das vítimas da rede Wi-Fi falsa para a rede autêntica, fazendo que

todos os recursos da rede Wi-Fi estejam disponíveis às vitimas. Após montar essa topologia, a estação do atacante passa a ser uma ponte entre a rede Wi-Fi autêntica e as vítimas, tendo plena capacidade de monitorar todo o tráfego pelo qual circula.

Wardriving

Wardriving é uma técnica de monitoramento de redes sem fio, utilizando dispositivos móveis, como *notebooks*, PDAs ou *smartphones*, para fazer essa varredura. A prática consiste em descobrir locais propícios à existência de redes sem fio em busca de redes abertas, sem nenhum protocolo de criptografia habilitado. Após a detecção das redes, é comum fazer marcações na calçada para informar as condições dessa rede. Essas marcações são padronizadas e recebem o nome de "*warchalking*".

É comum a utilização de antenas adicionais para a realização do *wardriving*, a fim de aumentar o alcance da varredura. Existem muitas antenas disponíveis no mercado, entretanto, a que parece ser a favorita para *wardriving* é uma antena caseira construída a partir da embalagem da batata Pringles.

Muitos não se contentam apenas em detectar essas redes sem fio com baixa segurança e acabam fazendo uso de serviços como a internet, pois dificilmente essa forma de acesso é detectada, principalmente por causa de dois fatores.

O primeiro é o acesso não ser feito por meio de provedor, pois o equipamento do invasor conecta-se diretamente à rede sem fio, o que torna seu rastreamento mais complicado de ser realizado.

O segundo fator que leva tantas pessoas a utilizarem essa forma de varredura é as redes sem fio não possuírem protocolos de criptografia habilitados e tenderem a não ser devidamente monitoradas pela equipe de suporte da empresa; caso contrário, essas redes seriam configuradas de maneira mais adequada.

Seguranças da Rede Wi-Fi

As redes Wi-Fi dispõem de uma série de ferramentas para sua proteção e de seus clientes conectados, tais como:

1) **Desabilitar o *broadcast* do SSID**: quando isso ocorre, a rede Wi-Fi torna-se oculta aos programas de conexão dessa rede Wi-Fi, entretanto, vários programas de monitoramento são capazes de detectar o SSID. Desabilitar o *broadcast* do SSID possibilita um aumento do nível de segurança.
2) **Filtro de MAC**: restringir o acesso à rede Wi-Fi apenas às estações com os endereços de MAC previamente cadastrados permite um controle maior sobre as estações que se conectam à rede. No entanto, esse método pode ser falho, uma vez que um atacante pode utilizar o endereço de uma estação previamente cadastrado para obter acesso à rede Wi-Fi.
3) **Isolamento do sinal rádio Wi-Fi**: sempre que possível, as redes Wi-Fi devem manter seus sinais de rádio dentro dos limites da corporação, evitando que a área de cobertura atinja locais que não deveria. Essa técnica muitas vezes não pode ser posta em prática, se considerarmos que diversas redes Wi-Fi normalmente são planejadas justamente para cobrir locais públicos, como os *shoppings*.
4) **802.1x**: método de autenticação que utiliza servidores *Radius* para validar usuários e senhas antes de disponibilizar acesso à rede Wi-Fi. Esse mecanismo de proteção agrega um alto nível de segurança a redes Wi-Fi.
5) **WPA2**: o WPA2 tem como objetivo substituir seus antecessores WEP e WPA. Até o momento, esse protocolo não apresentou falhas de segurança, se utilizado com chaves de segurança (*passphrases*) longas, isto é, de 8 a 63 caracteres.

11. QUESTÕES AUTOAVALIATIVAS

Confira, a seguir, as questões propostas para verificar o seu desempenho no estudo desta unidade:

1) Explique o principal fator que influencia a falta de segurança nas redes de comunicação.

2) Qual é o objetivo de utilizar a técnica de IP *spoofing* associada à de SYN *flood*?

3) Observando a Figura 3, explique como um *hacker* utiliza o mecanismo de inicialização de sessão do protocolo TCP (*three-way handshaking)* para consumir recursos de um servidor que comprometam sua disponibilidade.

4) Explique com suas palavras como são realizados os ataques DDoS.

5) Diferencie a técnica *smurf* de um ataque DDoS.

6) Cite os procedimentos indicados para se evitar as fraudes relacionadas à engenharia social.

7) Pesquise sobre os aplicativos disponíveis capazes de quebrar criptografias Wi-Fi, tais como *wepcrack*, WPA *crack* e *backtrack*. Compare cada um deles e indique suas principais características.

8) Cite e explique com suas palavras como as ferramentas de segurança da rede Wi-Fi podem ajudar a proteger um sistema computacional.

12. CONSIDERAÇÕES

Nesta unidade, você teve a oportunidade de conhecer como são originadas as principais ameaças a um sistema computacional, bem como técnicas a serem empregadas para elevar o nível de segurança.

Na próxima unidade, serão abordados mecanismos lógicos de controle de acesso que possibilitam uma ampla forma de configuração para atender a todos os níveis de segurança pretendidos.

13. REFERÊNCIAS BIBLIOGRÁFICAS

BURNETT, M. et al. *Maximum Windows 2000 Security*. Sams Publishing: [s.n.], 2001.

CARMONA, T.; HEXSEL, R. A. *Universidade Redes*: torne-se um especialista em redes de computador. São Paulo: Digerati Books, 2005.

CARUSO, C. A. A.; STEFFEN, F. D. *Segurança em informática e de informações*. 2. ed. rev. e ampl. São Paulo: Senac, 1999.

CHESWICK, W. R.; BELLOVIN, S. M.; RUBIN A. D. *Firewalls e segurança na internet*: repelindo o hacker ardiloso. 2. ed. Porto Alegre: Bookman, 2005.

GOUVÊA, S. *O direito na era digital*: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997.

KIZZA, J. M. *A guide to computer network security*. 2. ed. Tennessee: Springer, 2008.

LAUDON, K. C.; LAUDON, J. P. *Sistema de informações gerenciais*. 7. ed. São Paulo: Pearson Prentice Hall, 2007.

MAIWALD, E. *Fundamentals of network security*. Burr Ridge: McGraw-Hill Professional, 2003.

MARSHALL, I. W.; NETTLES S, M.; WAKAMIYA, N. (Ed.). Active networks. In: IFIP-TC6 THIRD INTERNATIONAL WORKING CONFERENCE, Iwan 2001, Philadelphia, PA, USA, September 30-October 2, 2001. *Proceedings*. Philadelphia: Springer, 2001.

MITNICK, K. D.; SIMON, W. L. *A arte de enganar*: ataques de hackers controlando o fator humano na segurança da informação. São Paulo: Pearson Education, 2003.

SCRIMGER, R.; LASALLE, P.; PARIHAR, M. *TCP/IP*: a bíblia. Rio de Janeiro: Elsevier, 2002.

EAD

Controles de Acesso Lógico

3

1. OBJETIVOS

- Identificar os controles de acesso lógico a serem implementados.
- Usar criptografia, assinatura e certificados digitais.
- Definir estratégias de segurança em uma rede por meio do conceito de *firewalls*.

2. CONTEÚDOS

- Criptografia.
- Assinatura digital.
- *Firewall*.

3. ORIENTAÇÕES PARA O ESTUDO DA UNIDADE

Antes de iniciar o estudo desta unidade, é importante que você leia as orientações a seguir:

1) Para saber mais sobre a prisão de Gottfried von Bismarck-Schönhausen, confira o *site* disponível em: <http://www.numaboa.com/criptografia/guerras-diplomacia/1244-bismarck-schonhausen>. Acesso em: 16 maio 2011.
2) Você encontrará boas informações sobre criptografia, técnica usada diversas vezes em períodos de guerra e nas comunicações feitas pelos serviços diplomáticos, no *site* disponível em: <http://www.numaboa.com/index.php?option=com_content&view=section&id=11&catid=57>. Acesso em: 8 maio 2011.
3) Para obter informações suplementares sobre os submarinos da Kriegsmarine, acesse o *site* disponível em: <http://www.numaboa.com/criptografia/guerras-diplomacia/1245-kriegsmarine>. Acesso em: 9 maio 2011.
4) Um exemplo de *software* que atua como *firewall* é o Comodo Firewall. Para mais informações, acesse o *site* do fabricante, disponível em: <http://www.comodobr.com/>. Acesso em: 5 jul. 2012.
5) Mark Abene é um dos maiores *hackers* da atualidade. Conheça mais sobre ele acessando o *site* disponível em: <http://exame.abril.com.br/revista-exame/edicoes/0641/noticias/conheca-o-hacker-phiber-optik-bandido-ou-mocinho-m0046272>. Acesso em: 16 abr. 2012.

4. INTRODUÇÃO À UNIDADE

Nas unidades anteriores, foram abordados os principais aspectos e políticas de segurança da informação, como também as ameaças às quais um sistema computacional está sujeito.

Nesta unidade, trataremos do desenvolvimento de estratégias cujo objetivo é o controle de tais sistemas computacionais, ou seja, abordaremos os principais mecanismos de controle de acesso lógico, capazes de garantir a proteção das informações, como criptografia, assinatura digital, certificado digital e *firewall*.

5. CRIPTOGRAFIA

Criptografia é a arte de escrever em códigos para esconder informações sob a forma de um texto incompreensível, intitulado "texto cifrado". O processo de codificação é chamado de "cifragem", e o processo inverso, o de descobrir o que há por trás do código inventado, é chamado de "decifragem".

Sem o conhecimento da chave correta, isto é, do valor do código secreto, não é possível decifrar um dado texto cifrado. Assim, basta manter a chave oculta, a fim de se obter uma segurança para o conteúdo da informação. Isso pode ser visto na Figura 1.

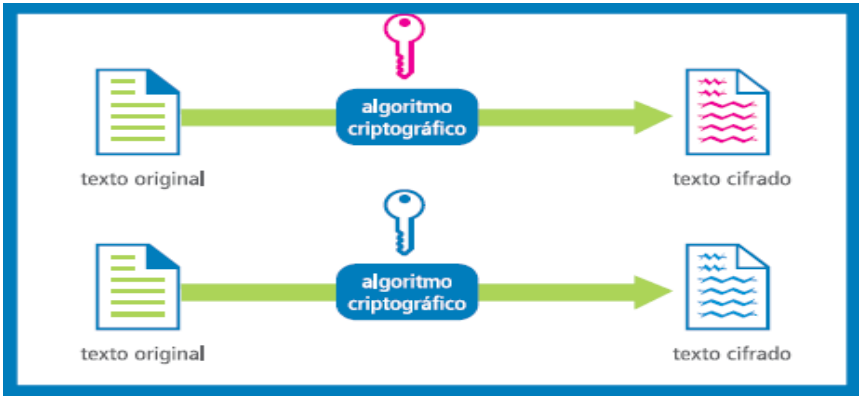


Figura 1 *Funcionamento da criptografia*.

O risco de se decifrar o texto e, consequentemente, a chave existe, e, por essa razão, as chaves devem ser frequentemente substituídas, implicando a possibilidade de interceptação ou captura do meio utilizado para a comunicação entre as partes.

A criptografia é conhecida desde a Antiguidade, quando era utilizada principalmente para fins de comunicações militares. Seu emprego comercial tornou-se amplo somente no final do século 20, quando passou a ser utilizada na comunicação e na proteção de dados confidenciais, por exemplo, em transações de transferência de valores bancários.

Os processos de criptografia tradicionais requerem um algoritmo criptográfico que, por meio de uma chave de cifragem, transforma um texto claro em um texto criptografado.

Conforme mencionado anteriormente, a necessidade de troca constante das chaves entre emissor e receptor pode implicar a vulnerabilidade do processo. Além do risco de interceptação, certamente a lista de chaves trocadas precisa ser armazenada em algum tipo de registro, também passível de posse não autorizada por terceiros.

Além do uso da técnica conhecida como "chave pública", existem outras formas de se contornar o problema apresentado anteriormente:

1) **Cifrar as chaves**: aumenta-se o grau de dificuldade para o atacante por meio da transmissão das chaves cifradas por um algoritmo diferenciado.
2) **Trocas frequentes de chaves**: a segurança cresce com essa troca, pois o atacante não sabe qual chave valerá para o momento. Em contrapartida, surgem os riscos envolvidos com a manutenção da lista de chaves de cifragem trocadas.
3) **Tamanho das chaves usadas**: quanto maior o tamanho, maior a garantia do processo, ou seja, reduz-se a possibilidade de decifração.
4) **Cifragens** múltiplas: submete a uma nova cifragem em relação às operações anteriores, aumentando a segurança do processo.
5) **Rotas alternativas**: pretende dificultar a captura do texto criptografado por meio de endereçamentos para outras portas, de um determinado *firewall* ou roteador.
6) **Cifragem cruzada**: nenhuma das partes conhece a chave utilizada pela outra. O emissor cifra a mensagem com uma chave somente do seu conhecimento. O receptor recebe a mensagem cifrada e realiza o mesmo procedimento, enviando a mensagem de volta ao emissor. O emissor decifra a mensagem com a chave original que usou para cifrá-la. A mensagem é, então, reenviada ao

receptor, agora protegida pela cifragem que ele executou. Por fim, a mensagem é decifrada pelo receptor. As desvantagens do processo são o tempo e o risco de interceptação, multiplicados por três, em virtude de envios e reenvios da mensagem.

7) **Redução do tamanho da mensagem**: quanto maior a mensagem, maior a quantidade de texto cifrado que o atacante terá para submeter à análise, facilitando, assim, a descoberta de padrões repetitivos que permitam estabelecer analogias. Reduzindo-se o tamanho das mensagens, reduz-se a possibilidade de interceptação, principalmente por causa da maior velocidade de transmissão.

Na atualidade, podemos destacar a criptografia simétrica e a criptografia assimétrica, essa última também denominada de "chave pública".

A criptografia simétrica é responsável pela cifragem de uma informação por meio de algoritmos que utilizam a mesma chave. "Troca de chaves" é a denominação do compartilhamento de uma chave conhecida.

No caso da criptografia assimétrica, algoritmos de chave pública operam com duas chaves diferentes, conhecidas como "chave privada" e "chave pública", que são geradas simultaneamente e relacionadas com a chave privada correspondente.

Para uma informação ser enviada de forma sigilosa, é necessário utilizar a chave pública do destinatário para codificar a informação, e, para que isso seja realizado com sucesso, é importante que o destinatário forneça sua chave pública. A Figura 2 exemplifica o que foi descrito até aqui.

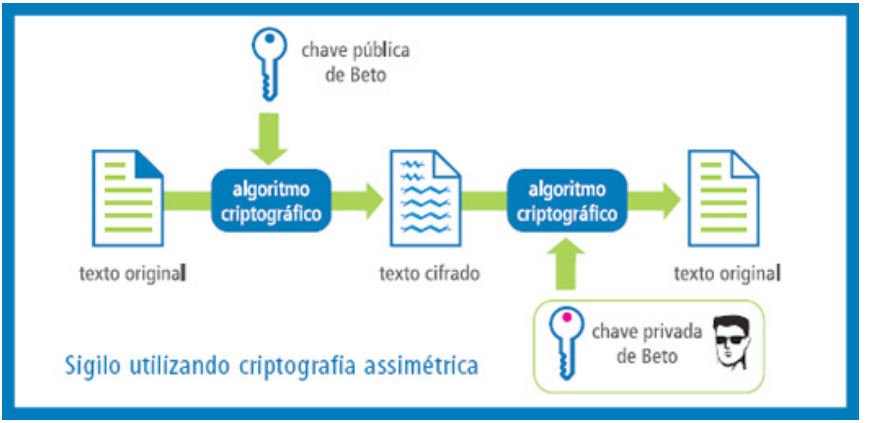


Figura 2 *Sigilo utilizando criptografia assimétrica*.

O sigilo pode ser considerado eficiente, pois somente o destinatário com a chave privada conseguirá desfazer a cifragem, isto é, poderá recuperar as informações iniciais. No caso da Figura 3, para Alice compartilhar algo de forma secreta com Beto (personagem apresentado na Figura 2), a informação precisa ser codificada, utilizando uma chave pública que Beto fornecerá. Assim, somente Beto pode decifrar a informação, pois apenas ele possui a chave privada correspondente.

No que diz respeito à autenticação, as chaves deverão ser utilizadas em sentido contrário ao da confidencialidade. Um exemplo disso está ilustrado na Figura 3.

Figura 3 *Autenticidade utilizando criptografia assimétrica*.

Caso uma informação seja cifrada com chave privada e, em seguida, enviada ao destinatário (nesse caso, Beto), este deverá decifrá-la, por possuir a chave pública do emissor (nesse caso, Alice). Entretanto, qualquer pessoa poderá decifrar a informação, uma vez que todos conhecem a chave pública de Alice. Em contrapartida, quando Alice utiliza uma chave privada para obter um texto cifrado, caracteriza uma ação que pode ser realizada somente por Alice, garantindo, assim, a autenticidade.

6. ASSINATURA DIGITAL

No campo da criptografia, a assinatura, ou firma digital, são formas de autenticação de informação digital análogas à assinatura em papel. Embora existam analogias, algumas diferenças importantes devem ser destacadas. Uma assinatura eletrônica faz referência a qualquer meio utilizado para identificar o emissor de uma mensagem eletrônica.

Ao utilizar uma assinatura digital, temos a comprovação de que certa mensagem foi enviada por um emissor. Observe que uma assinatura digital deve possuir as propriedades descritas a seguir:

- **Autenticidade**: quem recebe a assinatura deve ser capaz de verificar que ela foi realizada por um dado emissor.
- **Integridade**: caso a mensagem original sofra alguma alteração, a assinatura não corresponderá mais ao documento.
- **Não repúdio ou irretratabilidade**: um emissor não tem meios para reprovar a legitimidade de uma mensagem.

A forma de autenticação dos algoritmos de criptografia de chave pública atuando em conjunto com uma função *hash* (ou resumo) é intitulada "assinatura digital".

O retorno dado por uma função de *hash* (que é um resumo criptográfico) pode ser comparado a uma impressão digital, pois seu valor de resumo é único, e até mesmo a inserção de um espaço em branco ocasionará um resultado totalmente diferente do inicial.

Também deve ficar claro que apenas o código *hash* é cifrado utilizando a chave privada, como pode ser observado na Figura 4.

Figura 4 *Assinatura digital utilizando algoritmos de chave pública*.

Fazer uso de resumos criptográficos é melhor do que a utilização de algoritmos de criptografia assimétrica, em virtude da maior velocidade no processamento, pois os resumos possuem um tamanho menor que o documento.

Para validação de uma assinatura digital, é necessário, primeiramente, que o resumo criptográfico seja calculado a partir do documento original e a assinatura com chave pública do signatário seja decifrada. Em seguida, é preciso comparar o resumo criptográfico do documento original com o resultado da decriptação da assinatura digital, conforme pode ser visto na Figura 5. Se o resultado obtido for um valor igual, a assinatura é válida; caso contrário, a assinatura está incorreta.

Figura 5 *Conferência da assinatura digital*.

7. CRIPTOANÁLISE QUÂNTICA

A criptoanálise quântica tem como objetivo quebrar as técnicas usadas e tentar obter informações a partir de dados codificados sem ter acesso aos segredos requeridos pela decodificação normal.

A criptografia, em especial a assimétrica, é baseada atualmente na complexidade em solucionar alguns passos matemáticos. Essa complexidade é não polinomial, ou seja, mesmo utilizando uma chave de tamanho não muito grande, o tempo para solução ultrapassa os 100 anos, o que torna uma investida por força bruta quase impossível.

Com o surgimento da computação quântica, esses problemas podem ser resolvidos em menor tempo, pois ela se vale de vários tipos de testes simultâneos, ou seja, vários testes podem ser realizados ao mesmo tempo.

Essa inovação tecnológica colocaria em risco todas as formas e técnicas criptográficas utilizadas atualmente para quem possuir um computador quântico, o que torna necessário o desenvolvimento de novas técnicas de criptografia baseadas em algoritmos quânticos.

Por causa desse avanço, muitos países colocaram a criptografia como problema de segurança nacional e estão investindo cada vez mais na procura de uma nova forma de criptografar suas informações confidenciais.

A Criptografia RSA e o Algoritmo de Shor são dois tipos de computação quântica que veremos a seguir.

Criptografia RSA

A Criptografia RSA leva esse nome por causa de três professores do Instituto MIT: Ronald **R**ivest, Adi **S**hamir e Leonard

Adleman, inventores desse algoritmo. Trata-se da implementação de sistemas de chaves assimétricas fundamentado em teorias clássicas dos números.

É um tipo de criptografia de chave pública formado por duas chaves: uma codifica a mensagem e a outra decodifica. A chave que codifica é de conhecimento público, e a chave que decodifica é privada, ou seja, somente o administrador do sistema que recebe a mensagem será capaz de aplicar uma função na mensagem codificada e posteriormente lê-la. Dessa maneira, o RSA garante somente que o usuário legítimo seja capaz de decodificar a mensagem.

Algoritmo de Shor

O Algoritmo de Shor é muito conhecido e se vale da computação quântica. Com ele, é possível realizar a fatoração de números primos que possuem complexidade 0 ($\log^3 n$).

A seguir, os passos que o Algoritmo de Shor utiliza para fatorar um número qualquer múltiplo de dois primos (FRANCESE, 2011):

1) Aleatoriamente se escolhe um número *a* menor que N.
2) Calcula-se o Maior Divisor Comum (MDC) entre *a* e N. Se o resultado não for igual a 1, um dos fatores foi obtido.
3) Se o maior divisor for 1, ele calcula o período *r* da função $f(x) = a^x \bmod N$.
4) A computação quântica permite testar vários pares (x, *r*) simultaneamente, com uma probabilidade maior que ½ de encontrar um par válido.
5) Se *r* for ímpar ou se $a^{r/2} = -1$, retornar ao passo 1.
6) Um dos fatores desejados será o Maior Divisor Comum entre $a^{r/2} \pm 1$ e N.

8. CERTIFICADO DIGITAL

De acordo com o Boletim Tecnológico do TJPE (2011), o certificado digital é um documento eletrônico cuja função é de associar uma pessoa a uma chave pública. Ele normalmente apresenta as seguintes informações:

1) Nome da pessoa ou entidade a ser associada à chave pública.
2) Período de validade do certificado.
3) Chave pública.
4) Nome e assinatura da entidade que assinou o certificado.
5) Número de série.

Você observará que a Figura 6 apresenta um exemplo de certificado digital emitido pela Autoridade Certificadora Raiz Brasileira – ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira), que contém informações sobre o emissor do certificado e sua validade, entre outras.

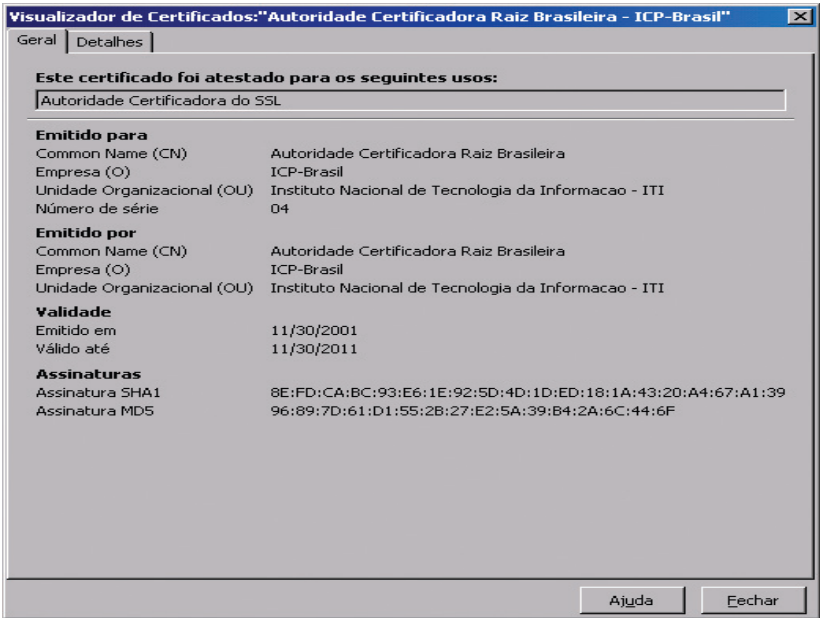


Figura 6 *Certificado digital da Autoridade Certificadora Raiz Brasileira – ICP-Brasil*.

Para verificação dos certificados instalados em seu computador, siga as instruções a seguir:

1) Verifique-os por meio do seu navegador.
2) No Internet Explorer, por exemplo, acesse o menu "Ferramentas", escolha "Opções da Internet".
3) Selecione a aba "Conteúdo".
4) Clique no botão "Certificados" e consulte os certificados na guia "Autoridades de Certificação Intermediárias".

Também podemos citar o uso da certificação digital em serviços governamentais, visando suportar as transações eletrônicas e proporcionando benefícios aos cidadãos, por exemplo, agilidade nas transações, redução da burocracia, entre outros.

Apesar das facilidades oferecidas pela certificação digital, faz-se necessário um alerta: o seu uso não torna as transações realizadas isentas de responsabilidades. Caso não haja proteção adequada para essas transações, tal como o antivírus, elas podem estar vulneráveis a ataques virtuais.

A seguir, apresentamos alguns tipos de vírus que podem atacar essas e outras operações.

9. VÍRUS E TIPOS DE AMEAÇAS

De forma semelhante à ação de um vírus biológico, temos o vírus de computador. Ele também infecta o sistema, faz cópias de si mesmo e tenta espalhar-se para outros computadores, utilizando-se de diferentes maneiras para isso.

O grande número de contaminações é dado pela ação do próprio usuário do computador infectado, que, de maneira inconsciente, executa arquivos infectados recebidos, na maioria das vezes, por *e-mails* ou *links* de acesso a páginas falsas ou de origem suspeita.

A infecção também ocorre por meio de arquivos infectados em *pen drives* ou CDs. Além disso, outro meio de infecção ocorre em razão da não instalação de correções de segurança lançadas para o sistema operacional, que, em sua grande maioria, tem o objetivo de corrigir vulnerabilidades existentes no sistema. Esses ataques normalmente são feitos por especialistas, como *hackers* e *crackers*.

A seguir, veremos a definição e a diferença entre eles.

Crackers e *hackers*

Muitos imaginam que as palavras *cracker* e *hacker* têm o mesmo significado, ou seja, que ambas caracterizam um mesmo perfil de pessoas, porém existe uma diferença entre elas.

Os *hackers* são aquelas pessoas que se dedicam à quebra de senhas, códigos e sistemas de segurança apenas por prazer próprio, não visando prejudicar outras pessoas. Já o *cracker* é um criminoso virtual, cuja intenção é roubar e extorquir pessoas utilizando os mais variados métodos no mundo virtual.

Nos próximos itens, veremos algumas das estratégias utilizadas para esses ataques, como o vírus de *boot*, o *time bomb*, o *worm* (também conhecido como "minhoca" ou "verme"), os *trojans*, ou cavalos de Troia, os *hijackers* e o estado zumbi.

Vírus de boot

O vírus de *boot* afeta a partição de inicialização do disco rígido, impossibilitando o carregamento do sistema operacional. Esse foi um dos primeiros tipos de vírus que surgiram.

Time bomb

O *time bomb* é um vírus pré-programado por seus criadores para entrarem em funcionamento em determinado dia e horário. Alguns desses vírus ficaram muito conhecidos como "Sexta-Feira 13", "Michelangelo", "Eros" e "1º de Abril" (*Conficker*).

Minhocas, worms, ou vermes

Os vermes, ou *worms*, têm apenas um objetivo, que é a replicação e espalhamento pela rede apenas para as criações ficarem conhecidas em toda a web, sem interesse de danificar o sistema. De forma geral, são mais evoluídos, pois, ao se hospedarem em uma dada máquina, conseguem se propagar na internet por meio de um cliente de *e-mail* instalado.

Trojans, ou cavalos de Troia

Determinados tipos de vírus trazem, em sua constituição, códigos à parte, que visam à coleta de dados ou acesso ao computador por um desconhecido na web sem que o usuário saiba o que está ocorrendo. Esses códigos são denominados de "*trojans*", ou "cavalos de Troia".

Hijackers

Os *hijackers* são programas mal-intencionados que alteram a página inicial do navegador da internet bloqueando qualquer tipo de mudança. Muitas vezes, são propagandas que surgem sem solicitação prévia do usuário em forma de *pop-ups*, instalação de barras de ferramentas, entre outros.

Estado zumbi

Quando infectado pelo estado zumbi, o computador é controlado por algum desconhecido, sem que o usuário saiba. Nos dias de hoje, é muito comum uma máquina ficar em estado zumbi, em razão do número elevado de fraudes existentes, especialmente bancárias, pois, quando o computador está nesse estado, é possível, para o controlador da máquina, roubar informações, como conta, senha, entre outras.

Veremos, a seguir, alguns tipos de proteção contra esses ataques, os *firewalls*.

10. FIREWALL

O *firewall* tem como objetivo reforçar a segurança nas comunicações estabelecidas entre as redes privadas e a internet, ou seja, busca evitar acessos indesejados às redes de dados privadas. No mercado atual, pode ser encontrado em duas plataformas, apresentando-se tanto como *hardware* dedicado quanto em *software*.

Ele atua na determinação dos serviços e/ou dados disponíveis nas redes privadas que podem ou não serem acessados por usuários de redes externas. Sua eficácia está diretamente relacionada à centralização de todo o tráfego entre a internet e a rede local, ou seja, todo o tráfego deve necessariamente passar por ele. As mensagens que trafegam entre essas duas redes distintas passam por uma verificação de segurança estabelecida pelo administrador da rede, e, caso ocorra alguma constatação de não cumprimento das regras de segurança, esse tráfego será bloqueado.

Em contrapartida, a utilização de *firewall* apresenta algumas limitações no aspecto de segurança, por exemplo, a incapacidade de proteger a rede privada dos próprios usuários internos, como também não é uma ferramenta eficaz contra vírus.

A Figura 7 ilustra um cenário em que um computador localizado fora da rede privada é capaz de realizar uma conexão com outro dispositivo por intermédio de um roteador. Uma vez estabelecida a conexão e não havendo qualquer mecanismo de controle de acesso, acessos indesejados aos dados podem ocorrer, ou seja, podem ser lidos, alterados ou, até mesmo, excluídos.

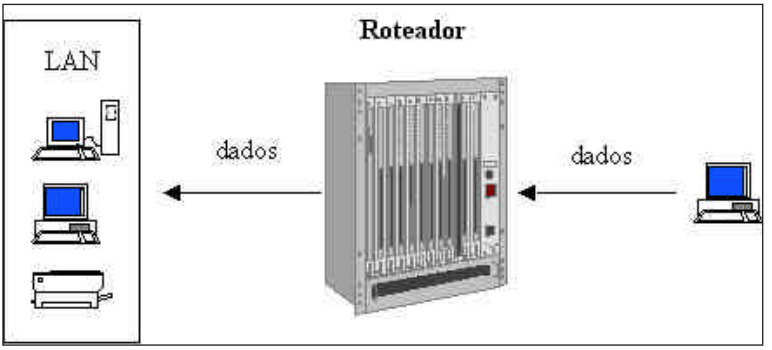


Figura 7 *O roteador permite o tráfego de informações entre computadores externos à LAN e os seus dispositivos, a princípio, sem qualquer tipo de segurança*.

Na tentativa de impedir os acessos indesejados citados anteriormente, é empregado o uso do *firewall*, que mantém a comunicação entre ambas as redes, desde que estejam autorizados em suas regras de segurança. No cenário inverso onde o tráfego é bloqueado, o *firewall* enviará uma mensagem ao computador de origem, informando a não conclusão da transmissão, mantendo, dessa maneira, a rede privada protegida de ataques externos.

A Figura 8 ilustra o tráfego autorizado entre um dispositivo externo e a rede privada ou local.

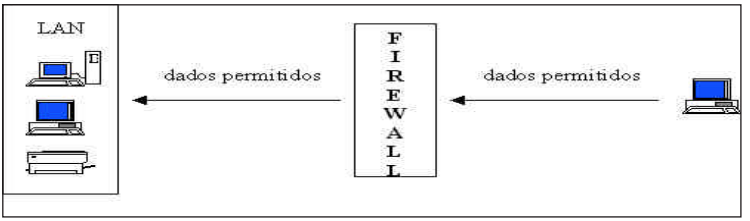


Figura 8 *Com a implementação do firewall, os dados continuam a ser transmitidos, desde que sejam permitidos*.

Já a Figura 9 mostra o tráfego não autorizado entre um dispositivo externo e a rede privada ou local.

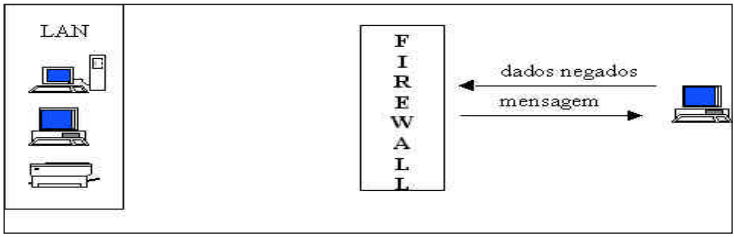


Figura 9 *Caso a transmissão dos dados seja negada pelo firewall, uma mensagem é transmitida para o computador externo à LAN, avisando que a transmissão não foi completada*.

Filtros de pacotes

Trata-se de uma técnica de filtragem de pacotes. Mais especificamente, são regras de avaliação que são aplicadas a todo pacote que entra no *firewall* e que decidem a permissão ou negação do tráfego. Tais regras de filtragem normalmente verificam os campos de um pacote, por exemplo, endereços IP de origem, endereços IP de destino, como também os números das portas TCP ou UDP utilizadas na comunicação.

Uma vez checados os campos citados, os filtros são capazes de distinguir entre pacotes que trafegam da rede interna para a internet ou vice-versa.

Apesar de a técnica de filtragem de pacotes ser efetiva e totalmente transparente ao usuário, é considerada vulnerável a ataques.

Gateways de aplicação

Outra técnica é o *gateway* de aplicação. O *gateway* é um dispositivo que oferece serviços de transmissão de dados entre duas redes. Os *firewalls*, como já visto, não são capazes de realizar a filtragem de conexões para serviços, como TELNET e FTP, função essa atribuída aos *gateways* de aplicação. Ambas as técnicas (*firewall* e *gateway* de aplicação) normalmente devem trabalhar em conjunto, visando níveis mais elevados de segurança.

Os *gateways* de aplicação apresentam algumas vantagens sobre o controle tradicional do tráfego entre redes privadas e a internet, incluindo o mecanismo capaz de esconder informação, isto é, informações das redes privadas não são divulgadas para as redes externas, pois estas somente visualizam o *gateway*.

Os componentes de um *gateway* de aplicação são ilustrados na Figura 10.

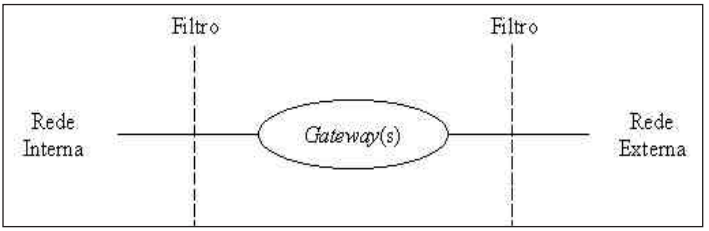


Figura 10 *Componentes de um gateway de aplicação*.

Servidores *proxy*

O *proxy* é um servidor configurado para atender as requisições de um cliente a um serviço. A disponibilização dos recursos ao cliente pode se dar mesmo sem a efetiva conexão com o servidor especificado, armazenando dados localmente, o chamado "*cache*".

Recomenda-se que os servidores *proxy* sejam instalados em equipamentos (servidores) com alto poder de processamento e armazenagem de dados.

Melhoria de desempenho

Uma das vantagens de utilização de *proxy* é a melhoria de desempenho, pois os pedidos feitos pelo usuário ao servidor são armazenados por um determinado período. Assim, se uma nova requisição for solicitada e já estiver armazenada nos registros do servidor de *proxy*, o acesso é dado de forma bem mais rápida.

11. QUESTÕES AUTOAVALIATIVAS

Confira, a seguir, as questões propostas para verificar o seu desempenho no estudo desta unidade:

1) Explique como funciona um algoritmo de criptografia de chave pública.

2) O que é a função *hash*? Disserte sobre o processo de criptografia em assinatura digital.

3) Explique com suas palavras os princípios da criptografia quântica. Quais mudanças ela apresenta para o futuro da segurança digital?

4) Além do emprego na transmissão de dados, em que outro cenário você utilizaria a criptografia?

5) Pesquise o significado e as funções da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira).

6) O que é um certificado digital? Dê um exemplo em que ele é amplamente utilizado.

7) Ao utilizarmos um serviço bancário *on-line,* é feito o uso de certificado digital? Justifique sua resposta.

8) Explique resumidamente como um vírus pode infectar um computador. Liste quais são os tipos de ameaça. Escolha duas ameaças e explique-as resumidamente.

9) Discorra sobre o funcionamento de um *firewall*.

10) O que é um *proxy*? Como é o seu funcionamento?

11) Qual a diferença básica entre um *firewall* e um *proxy*?

12. CONSIDERAÇÕES

Nesta unidade, aprendemos a identificar os controles de acesso lógico a serem implementados em cada cenário de ataque possível, como, por exemplo, o uso de assinatura digital e criptografia. Além disso, foram abordados os principais conceitos de *firewall*, ou seja, definições e estratégias de segurança em uma rede por meio desse conceito.

A partir da próxima unidade, estudaremos os processos envolvidos na auditoria da Tecnologia da Informação. Nesse cenário, serão discutidos aspectos referentes à metodologia, aos requisitos de conformidade e às medidas de contingência de um sistema de informação.

13. E-REFERÊNCIAS

Lista de figuras

Figura 1 *Funcionamento da criptografia*. Disponível em: <http://yross.wordpress.com/2010/07/13/criptografia-digital/>. Acesso em: 31 ago. 2011.

Figura 2 *Sigilo utilizando criptografia assimétrica*. Disponível em: <http://yross.wordpress.com/2010/07/13/criptografia-digital/>. Acesso em: 31 ago. 2011.

Figura 3 *Autenticidade utilizando criptografia assimétrica*. Disponível em: <<http://yross.wordpress.com/2010/07/13/criptografia-digital/>. Acesso em: 31 ago. 2011.

Figura 4 *Assinatura digital utilizando algoritmos de chave pública*. Disponível em: <http://yross.wordpress.com/2010/07/13/criptografia-digital/>. Acesso em: 31 ago. 2011.

Figura 5 *Conferência da assinatura digital*. Disponível em: <http://yross.wordpress.com/2010/07/13/criptografia-digital/>. Acesso em: 31 ago. 2011.

Figura 6 *Certificado digital da Autoridade Certificadora Raiz Brasileira – ICP Brasil*. Disponível em: <http://www.tjpe.gov.br/Boletim/N41/dicadahora03.htm>. Acesso em: 2 set. 2011.

Figura 7 *O roteador permite o tráfego de informações entre computadores externos à LAN e os seus dispositivos, a princípio, sem qualquer tipo de segurança*. Disponível em: <http://www.rederio.br/downloads/pdf/roteador.pdf>. Acesso em: 2 set. 2011.

Figura 8 *Com a implementação do firewall, os dados continuam a ser transmitidos, desde que sejam permitidos*. Disponível em: <http://www.rederio.br/downloads/pdf/roteador.pdf>. Acesso em: 2 set. 2011.

Figura 9 *Caso a transmissão dos dados seja negada pelo firewall, uma mensagem é transmitida para o computador externo à LAN, avisando que a transmissão não foi completada*. Disponível em: <http://www.rederio.br/downloads/pdf/roteador.pdf>. Acesso em: 2 set. 2011.

Figura 10 *Componentes de um gateway de aplicação*. Disponível em: <http://www.rederio.br/downloads/pdf/roteador.pdf>. Acesso em: 2 set. 2011.

Sites pesquisados

FRANCESE, J. P. S. *Criptoanálise quântica*. Aplicações. Disponível em: <http://www.gta.ufrj.br/grad/08_1/quantica/cap3.html#sub2>. Acesso em: 5 set. 2011.

ISIDRO, C. R. G. *Introdução à criptografia clássica e* à criptografia quântica. Disponível

em: <http://www.dsc.ufcg.edu.br/~gmcc/mq/criptografia.html>. Acesso em: 25 maio 2011.

TJPE. *Boletim tecnológico*. Certificado digital. Disponível em: <http://www.tjpe.gov.br/Boletim/N41/dicadahora03.htm>. Acesso em 31 ago. 2011.

14. REFERÊNCIAS BIBLIOGRÁFICAS

COMER, D. E. *Redes de computadores e internet*. 4. ed. Porto Alegre: Bookman, 2007.

KUROSE, J. F. *Redes de computadores e a internet*: uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

EAD

Auditoria da Tecnologia da Informação

4

1. OBJETIVOS

- Estabelecer os critérios para a definição de uma equipe de auditoria e uma área a ser auditada, estabelecendo metodologias e procedimentos a serem adotados.
- Planejar a execução de uma auditoria.
- Elaborar um relatório final de auditoria.

2. CONTEÚDOS

- Metodologia para auditoria de sistemas.
- Requisitos de conformidade.
- Relatórios.
- Medidas de contingência.

3. ORIENTAÇÕES PARA O ESTUDO DA UNIDADE

Antes de iniciar o estudo desta unidade, é importante que você leia as orientações a seguir:

1) De forma objetiva e buscando alinhar os conceitos teóricos ao cotidiano prático, esta unidade apresenta as metodologias e os procedimentos a serem adotados em um processo de auditoria, seu planejamento e execução, bem como traz o conceito de relatórios escritos da auditoria, sempre visando o desenvolvimento de seu aprendizado.
2) Antes de iniciar os estudos desta unidade, sugerimos a leitura das reportagens disponíveis nos *sites* a seguir, pois elas abordam assuntos atuais e pertinentes. Boa leitura!
    a) AZEREDO, P. *Auditores de TI buscam espaço*. Disponível em: <http://www.timaster.com.br/revista/materias%5Cmain_materia.asp?codigo=1142>. Acesso em: 12 maio 2011.
    b) BRASILIANO, A. C. R. *ERM Enterprise Risk Management, reinvenção no seu conceito*. Disponível em: <http://www.faculdadedeengenharia.com/?p=518>. Acesso em: 12 maio 2011.
    c) UOL NOTÍCIAS. *Visão estratégica é um dos principais desafios para os auditores internos*. Disponível em: <http://economia.uol.com.br/planodecarreira/ultnot/infomoney/2009/08/20/ult4229u2809.jhtm>. Acesso em: 12 maio 2011.

4. INTRODUÇÃO À UNIDADE

Na unidade anterior, você estudou os principais mecanismos de controles de acesso lógico que buscam garantir ou ao menos minimizar os incidentes causados por quebra de segurança. Nesta unidade, você estudará os aspectos mais importantes relacionados à auditoria da Tecnologia da Informação (TI).

Em virtude do alto número de recursos de TI utilizados dentro das empresas, tem sido necessário um maior controle sobre as áreas de TI, denominado "auditoria".

A auditoria de sistemas é responsável pela revisão e avaliação dos controles do sistema de informação. Seu objetivo é manter a autenticidade e a integridade dos dados, além de proteger os ativos da organização.

No centro de processamentos de dados, a auditoria deve abranger as seguintes áreas da TI:

1) Recuperação de desastre.
2) Capacidade dos sistemas.
3) Desempenho dos sistemas.
4) Desenvolvimento de sistemas.
5) Sistemas financeiros.
6) Rede de telecomunicações.
7) Segurança de informação.

Vamos ao estudo!

5. CONCEITOS E ORGANIZAÇÃO DA AUDITORIA

O que é auditoria?

A auditoria é uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o objetivo de verificar sua conformidade com certas políticas institucionais, normas e padrões.

O principal foco de uma auditoria é descobrir irregularidades dentro das empresas, buscando identificar os problemas para, em seguida, traçar a melhor estratégia para resolvê-los.

Uma das peças mais importantes dentro da auditoria é o auditor. Ele deve ser capaz de raciocinar objetiva e logicamente, além de necessariamente possuir um vasto conhecimento na área de TI.

Fases da auditoria

A atividade de auditoria pode ser dividida em três fases:

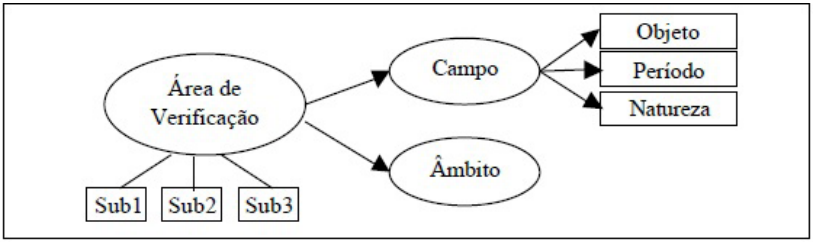
1) planejamento;
2) execução;
3) relatório.

Planejamento e execução

A fase de planejamento de uma auditoria diz respeito a instrumentos imprescindíveis para a sua realização. Para isso, faz-se necessário: estudo preliminar e elaboração e aprovação do plano anual de auditoria.

Segundo Dias (2002), o contexto da auditoria baseia-se em três pilares: o objeto (foco da auditoria), o período e a natureza da auditoria. O objeto é a organização ou instituição (pública ou privada), e o período é a quantidade de tempo (determinado por uma data e/ou hora inicial e final), como, por exemplo, um mês, um ano ou até mesmo um período completo da gestão de determinado gerente.

Observe, na Figura 1, que a área de verificação é o conjunto formado por campo e âmbito de auditoria.



Fonte: Dias (2000, p. 108).
Figura 1 *Área de verificação*.

Para um bom planejamento, faz-se necessário definir os motivos ou as naturezas da auditoria.

Os motivos ou as naturezas da auditoria apresentam-se agrupados quanto:

1) Ao órgão fiscalizador:
   a) auditoria interna: realizada por um departamento da própria empresa e tem como objetivo a diminuição de erros e fraudes.
   b) auditoria externa: realizada por uma empresa sem vínculo com a empresa auditada e tem como objetivo avaliar a gestão da empresa, seja financeiramente, seja operacionalmente.
   c) auditoria articulada: é uma junção das auditorias externas e interna.
2) À forma de abordagem do tema:
   a) auditoria horizontal;
   b) auditoria orientada.
3) Ao tipo ou à área envolvida:
   a) auditoria de programas de governo;
   b) auditoria de planejamento estratégico;
   c) auditoria administrativa;
   d) auditoria contábil;
   e) auditoria financeira, ou auditoria das contas;
   f) auditoria da legalidade;
   g) auditoria operacional;
   h) auditoria integrada;
   i) auditoria de TI: especificamente realizada de forma operacional, em que são avaliados os sistemas e a segurança de informações, realizando o apontamento e a instrução para correções de eventuais erros que sejam identificados.

O controle é uma forma de fiscalizar pessoas, setores e órgãos de uma determinada empresa. Os tipos de controle podem ser:

- preventivos: responsáveis pela prevenção de erros e atos de fraude dentro de uma empresa;

- detectivos: responsáveis pela detecção de erros e atos de fraude dentro de uma empresa;
- corretivos: responsáveis pela correção dos erros detectados dentro de uma empresa.

A segunda fase da auditoria de sistemas está relacionada à execução propriamente dita da auditoria.

A auditoria de sistemas é responsável pela avaliação dos recursos existentes no tocante à TI, procurando avaliar quesitos principais, como eficiência e eficácia. Analisa o ambiente de forma geral, desde a segurança física até a segurança lógica.

É possível também na auditoria de sistemas realizar a gestão sobre banco de dados, redes de dados e desenvolvimento de *softwares*.

Segue a classificação quanto às subáreas:

- Auditoria da segurança de informações: responsável pelos controles de acesso lógicos, controles de acesso físicos, controles ambientais e plano de contingências.
- Auditoria da TI: envolve tudo que foi citado em auditoria da segurança de informações, além de abranger controles organizacionais, controle de banco de dados, controle de microcomputadores e controle sobre cliente servidor.
- Auditoria de aplicativos: diz respeito ao controle sobre desenvolvimento de *software*, controle de processamento de dados e controle sobre funcionalidade de aplicativos.

A pessoa que toma a frente de uma equipe de auditoria deve ter capacidade para formar um profissional ou recrutá-lo com capacitação técnica para um processo de auditoria em âmbito de TI.

Cada pessoa formada ou recrutada da equipe deve possuir plenos conhecimentos e experiência na área de TI e já ter, de preferência, participado de alguma auditoria do tipo.

Em alguns casos de auditoria, talvez sejam necessários conhecimentos além dos exigidos em TI, ou seja, conhecimentos mais específicos, como CAATs (*Computer Assisted Audit Techniques*), que é um programa utilizado em auditoria para extrair dados e linguagens de programação específicas.

Relatórios

Por fim, a terceira fase da auditoria de sistemas trata da elaboração de relatórios escritos, na qual são pontuados os principais aspectos identificados no processo, conforme detalhado a seguir.

O objetivo de se elaborar um relatório de forma escrita é registrar as conclusões chegadas após todo o processo de auditoria, e o relatório pode conter várias comprovações, contanto que sejam bem explicadas e com o uso de linguagem técnica.

O relatório final deve ser lido e revisado por todos os auditores envolvidos no processo de auditoria e aprovado para que tenha validade. Também deve sofrer uma revisão textual, para excluir eventuais erros gramaticais.

É interessante que a estrutura do relatório final possua os seguintes itens: dados da entidade que sofreu auditoria, um resumo do conteúdo, dados da equipe formada para auditoria, uma breve introdução com os departamentos auditados, o apontamento das falhas detectadas ao longo do processo de auditoria, um conclusão sobre o processo e, finalmente, o parecer da gerência superior.

6. METODOLOGIA PARA AUDITORIA DE SISTEMAS

Definido o tipo de equipe, a organização pode prosseguir com a auditoria, adotando as metodologias possíveis: entrevistas e Uso de Técnicas ou Ferramentas de Apoio (CAATs). Vejamos cada um delas.

Entrevistas

Durante a auditoria, entrevistas podem ser feitas com os funcionários da organização, apresentando o plano da auditoria que será realizado, coletando dados, identificando falhas e irregularidades.

Essas entrevistas podem ser:

1) Entrevista de apresentação: a ser realizada com os gerentes, funcionários e diretores, com o objetivo de apresentar o plano de auditoria, cronograma de atividades, solicitação de salas, armários, mesas, entre outros objetos.
2) Entrevista de coleta de dados: é realizada com o intuito de coletar dados sobre o sistema e ambientes de informática. Nessa entrevista, podem ser identificados alguns pontos críticos e possíveis irregularidades, sem coação do entrevistado por parte do auditor, mostrando a ele o resultado final para evitar problemas.
3) Entrevista de discussão das deficiências encontradas: são discutidos abertamente os pontos críticos, e justificativas são apresentadas para tais falhas. É uma forma interativa que dá oportunidade ao auditado de expor seus pontos de vista. Nem sempre as auditorias permitem essa discussão.
4) Entrevista de encerramento: ao final do trabalho, é realizada uma reunião com os dirigentes da entidade auditada para agradecimentos à colaboração da direção e funcionários e com apresentação dos resultados da auditoria, recomendações, comentários e entrega dos relatórios.

Uso de Técnicas ou Ferramentas de Apoio (CAATs)

Outra metodologia é o Uso de Técnicas ou Ferramentas de Apoio (CAATs). Os auditores podem utilizar a informática para realizar suas tarefas, as quais são divididas nas seguintes categorias:

- Análise de dados: realiza-se a análise de dados coletados por meio de *softwares* e dos *logs* retirados da auditoria.
- Verificação de sistemas: averiguam-se, por intermédio de testes, a funcionalidade e a confiabilidade dos sistemas que estão sofrendo auditoria.

7. MEDIDAS DE CONTINGÊNCIA

Um plano de contingência e de recuperação de desastres apresenta medidas operacionais estabelecidas e documentadas para serem seguidas no caso de ocorrer alguma indisponibilidade dos recursos de informática, evitando-se que o tempo no qual os equipamentos ficaram parados acarrete perdas materiais aos negócios da empresa.

O plano de continuidade, como conhecido, numa visão secundária, é mais que somente recuperação das atividades de informática. Contempla, também, as preocupações concernentes à vida dos funcionários, aos impactos sobre meio ambiente, às imagens em relação aos clientes, fornecedores e público em geral.

Quando o ambiente for muito complexo, a responsabilidade básica é da diretoria da área de TI. Se o ambiente for moderado, o responsável é o gerente de TI, e, se o ambiente for mais simples, a responsabilidade recai sobre o encarregado ou os analistas de sistemas responsáveis pela administração da rede. No entanto, para que as medidas de contingência sejam efetivas, a alta direção precisa apoiar as medidas, visto que elas têm intuito estratégico.

Ao programá-lo, efetivamente, deve-se estabelecer os responsáveis pela consecução das ações de contingência. Normalmente, as pessoas designadas para assumirem ações de contingências no momento de desastres são pessoas diferentes daquelas que executam funções operacionais no dia a dia em ambiente de TI. Para evitar conflitos, as responsabilidades são delineadas, documentadas e colocadas à disposição do grupo chamado de "equipe de contingência".

A disponibilização dos dados é de vital importância para o *workflow* dos sistemas das empresas. Por isso, a adoção de um plano de contingência visa garantir a busca e a transformação desses dados sem causar descontinuidade operacional da empresa, em caso da quebra de equipamentos ou ocorrência de algo não planejado.

No processo de implementação do plano de contingência, é recomendado que o usuário se avalie quanto ao nível de risco a que está sujeito, observando a importância de sua atividade para as funções críticas dos negócios, as quais se enquadram numa das três categorias a seguir:

1) Alto risco.
2) Risco intermediário.
3) Baixo risco.

Após essa avaliação, o usuário deve verificar que tipo de proteção é a mais recomendada para cada uso.

Objetivos da auditoria de plano de contingência e recuperação de desastres

Os objetivos da avaliação dos planos de contingência de uma empresa são certificar-se de que:

1) Há planos desenvolvidos que contemplam todas as necessidades de contingências.
2) Esses planos são suficientemente abrangentes para cobrir aspectos físicos, lógicos, de rede, de propriedades intelectuais, de pessoas, transacionais, entre outros.
3) A equipe de contingência está preparada para as eventualidades.
4) Esses planos são testados periodicamente.
5) Os *backups* são atualizados.
6) Os mesmos *backups* podem ser recuperados com pouca ou nenhuma dificuldade.
7) Há relatórios gerenciais que facilitam o acompanhamento dos procedimentos.
8) Os relatórios são confiáveis.

Exemplo de plano de contingência

Serão abordados apenas casos com níveis de riscos altos ou intermediários em ambiente de rede operada pelas empresas médias.

A seguir, os itens contemplados nesse plano de contingência:

1) Classificação das aplicações críticas.

   Geralmente, as empresas industriais costumam estabelecer as seguintes aplicações mais críticas:

   a) Sistemas de Faturamento/Contas a Receber.
   b) Sistemas de Compras/Contas a Pagar.
   c) Sistemas de Recursos Humanos/Folha de Pagamento.
   d) Sistemas de Estoques/Custo de Produção.
   e) Sistemas de Contabilidade Geral.

2) Contingência em relação aos recursos tecnológicos.

   Para esse caso específico, havendo indisponibilidade, existe um contrato de manutenção, quando a empresa contratada se responsabiliza em colocar outro equipamento semelhante dentro de um prazo de tempo mínimo, no qual a inatividade operacional da empresa não passe a interferir no seu funcionamento:

   a) Utilização de servidores da área industrial conforme negociado.
   b) Capacitação dos servidores nos requerimentos mínimos de *hardware*, conforme o tipo de servidor (rede ou banco de dados).
   c) Substituição dos *switches* ATM por Ethernet.
   d) Manutenção da estrutura de rede em padrão Ethernet.
   e) Restauração dos *backups* dos servidores com os dados mais atuais, conforme política de *backup*.

f) Ativação do CPD temporário na área de informática, ou, em caso da indisponibilidade da área, utilização do local disponível mais apropriado.

3) Contingência em relação aos aplicativos críticos.

No caso de indisponibilidade das linhas telefônicas por períodos prolongados e não suportados, deverão ser tomadas as seguintes medidas em relação aos sistemas:

a) Sistemas de Faturamento/Contas a Receber.
   - Emissão de notas fiscais em São Caetano do Sul.
   - Emissão manual de nota fiscal.
   - Utilização de *hotsite* já cadastrado.

b) Sistemas de Compras/Contas a Pagar
   - Solicitações de compras e pagamentos feitos manualmente.
   - Utilização do *hotsite* já contratado.

c) Sistemas de Contabilidade Geral
   - Os lançamentos deverão ser feitos no *hotsite* já cadastrado.
   - Utilização do centro de processamento de dados de São Caetano do Sul.

d) Sistema de Recursos Humanos/Folha de Pagamento
   - Utilização do centro de processamento de dados de São Caetano do Sul.
   - Utilização do *hotsite* se for necessário.

8. EXEMPLO DE RELATÓRIO DE AUDITORIA

Depois de compreendidas as fases que envolvem o processo de auditoria (planejamento, execução e relatório), no *link* apresentado a seguir, pode ser verificado um exemplo de Relatório de Auditoria, para maior fixação dos conceitos teóricos: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2056494.PDF>. Acesso em: 27 jun. 2012.

É de fundamental importância o acesso a esse *link* e a leitura de alguns trechos do relatório, pois, dessa forma, ficará mais claro como ocorreu a auditoria e como são apresentadas formalmente todas as conclusões e revisões para a empresa auditada.

Muitos defendem o surgimento da auditoria desde os primórdios das sociedades, porém não é possível provar tal fato. Com esse raciocínio, é quase um crime não existir auditorias no atual cenário econômico, por causa do crescimento do mercado de forma constante e acelerada.

Ao longo do tempo, muitas mudanças foram realizadas para chegarmos ao atual cenário de importância ocupado pela auditoria.

Um dos exemplos a serem citados é a criação do Instituto Americano de Contadores Públicos Certificados, que é um órgão regulamentado responsável pela publicação de padrões profissionais e guias de recomendações.

É possível a extração de muito conhecimento ao se estudar a fundo esta área, que vem se tornando uma das principais em todo o mundo.

9. QUESTÕES AUTOAVALIATIVAS

Confira, a seguir, as questões propostas para verificar o seu desempenho no estudo desta unidade:

1) O que é uma auditoria de sistema e quais seus objetivos?

2) Dentre os vários tipos de auditoria, explique detalhadamente dois deles.

3) Quais são as fases de um processo de auditoria? Elabore uma breve explicação sobre cada uma dessas fases.

4) Existem algumas organizações de certificação de qualificação profissional para auditoria. Faça uma pesquisa das principais organizações responsáveis por essa certificação.

5) Explique, com base em metodologia para auditoria de sistemas, como devem ser realizadas as entrevistas com os funcionários.

6) Explique resumidamente como deve ser um relatório de auditoria e qual a estrutura que um relatório deve possuir.

7) O que são medidas de contingência e qual sua importância em um âmbito empresarial?

8) Quais são os objetivos da auditoria de plano de contingência?

9) Com base no exemplo dado no Tópico 8, quais são as medidas mais importantes de contingência que devem ser tomadas, tanto em relação aos recursos tecnológicos quanto aos aplicativos?

10. CONSIDERAÇÕES

Nesta unidade, estudamos as metodologias para definição de uma equipe de auditoria e a área a ser auditada. Também foram abordados aspectos do planejamento e execução de uma auditoria do sistema de informação.

Encerramos a unidade discutindo a importância dos relatórios elaborados, contendo as conclusões do processo de auditoria, além das medidas e planos de contingência.

Uma vez apresentados tais fundamentos, na próxima unidade, trataremos das práticas de Governança de TI, demonstrando os principais modelos de boas práticas, como COBIT e ITIL.

11. REFERÊNCIAS BIBLIOGRÁFICAS

DIAS, C. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books, 2000.

IMONIANA, J. O. *Auditoria de sistemas de informação*. 2. ed. São Paulo: Atlas, 2005.

EAD

Governança de Tecnologia da Informação

5

1. OBJETIVOS

- Conceituar Governança de Tecnologia da Informação (TI).
- Avaliar os modelos de melhores práticas.
- Analisar como as melhores práticas de governança se relacionam.
- Verificar os resultados da implantação dos modelos de melhores práticas em organizações.

2. CONTEÚDOS

- Aspectos da metodologia COBIT.
- Aspectos da metodologia ITIL.

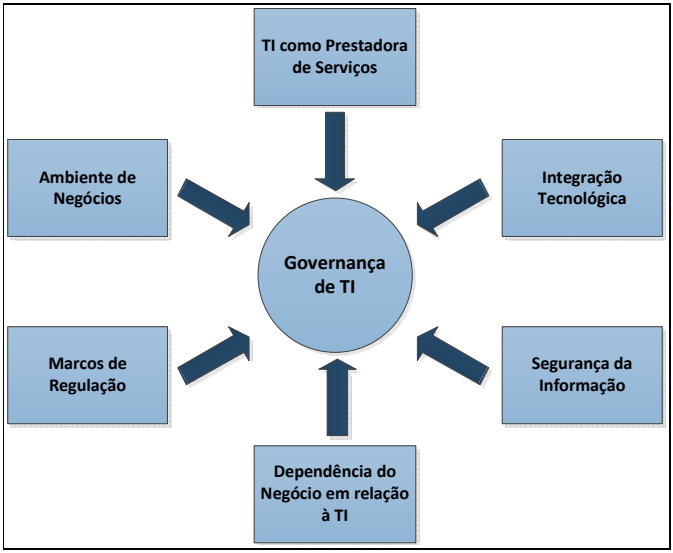
3. ORIENTAÇÕES PARA O ESTUDO DA UNIDADE

Antes de iniciar o estudo desta unidade, é importante que você leia as orientações a seguir:

1) Recomendamos o acompanhamento das atualizações dos modelos de boas práticas do mercado por meio do acesso a *sites* disponíveis, por exemplo, em: <http://www.isaca.org> e <http://www.itil-officialsite.com>. Acesso em: 27 maio 2011.
2) Ressalte-se que o objetivo principal deste *Caderno de Referência de Conteúdo* é capacitá-lo para ser um gestor da informação com conhecimentos sobre segurança e auditoria de sistemas. Assim, para que o processo de aprendizado se solidifique, faz-se necessário que você compreenda bem os conceitos e as perspectivas praticadas no processo de implantação da Governança de TI dentro das organizações.
3) As Normas ISO 17.799 e ISO 27.001 são provavelmente as mais conhecidas sobre segurança da informação. Para mais informações a respeito dessas normas, sugerimos a leitura da obra *Sistema de segurança da informação: controlando os riscos*, de André Campos.
4) Proponha-se a buscar novos conhecimentos acerca dos demais modelos de melhores práticas oferecidos pelo mercado, bem como, se julgar interessante e for possível, a realizar treinamentos e, posteriormente, exames de certificação dos produtos. Lembrando que os profissionais certificados são reconhecidos pelas organizações como aptos a colocar em prática o conhecimento adquirido, e, além disso, a certificação influencia diretamente no processo de contratação, como também na remuneração do profissional.

4. INTRODUÇÃO À UNIDADE

Vários são os motivadores da Governança de TI, como pode ser observado na Figura 1, porém o fator que mais se destaca é a transparência da administração.



Fonte: Fernandes e Abreu (2008, p. 8).
Figura 1 *Fatores motivadores da Governança de TI*.

Conforme descrito por Fernandes e Abreu (2008, p. 175), o IT Governance Institute (2005) define que:

> A governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização.

Podemos concluir que a Governança de TI busca o envolvimento dos demais dirigentes da organização em suas decisões e de como os seus serviços serão providos à empresa. Dentro desse contexto, surge o que chamamos de **Ciclo da Governança de TI**, composta por quatro etapas distintas:

1) Alinhamento estratégico.
2) Decisão, compromisso, priorização e alocação de recursos.
3) Estrutura, processos, operações e gestão.
4) Medição do desempenho.

A primeira etapa do Ciclo da Governança de TI apresenta o seu principal objetivo, ou seja, alinhar TI aos requisitos do negócio.

Para tal, existem, atualmente, vários modelos de melhores práticas para TI, conforme ilustrado no Quadro 1.

Quadro 1 Principais modelos de melhores práticas.

MODELO DE MELHORES PRÁTICAS	ESCOPO DO MODELO
COBIT – *Control Objectives for Information and related Technology*	Modelo abrangente aplicável para a auditoria e controle de processos de TI, desde o planejamento da tecnologia até a monitoração e auditoria de todos os processos.
VAL IT	Modelo para a gestão do valor e investimentos de TI.
CMMI – *Capability Maturity Model Integration (for Development)*	Desenvolvimento de produtos e projetos de sistemas e *software*.
ITIL – *Information Tecnology Infrastructure Library*	Infraestrutura de tecnologia da informação (definição da estratégia, desenho, transição, operação e melhoria contínua do serviço).
ISO/IEC 27001 e ISO/IEC 27002 – Código de prática para gestão da segurança da informação	Segurança da Informação.
MODELOS ISO – *International Organization for Standardization*	Sistemas da qualidade, ciclo de vida de *software*, teste de *software* etc.
The eSourcing Capability Model for Service Providers (eSCM-SP)	*Outsourcing* em serviços que usam TI de forma intensiva.
The eSourcing Capability Model for Client Organizations (eSCM-CL)	Conjunto de práticas para que o cliente defina a estratégia e o gerenciamento do *outsourcing* de serviços de TI ou fortemente baseados em TI.
PRINCE2 – *Project in Controlled Environments*	Metodologia de gerenciamento de projetos.
P3M3 – *Portfolio, Programme & Project Management Maturity Model*	Modelo de maturidade para o gerenciamento de projetos, programas e *portfolio.*
PMBOK – *Project Management Body of Knowledge*	Base de conhecimento em gestão de projetos.
OPM3 – *Organizational Project Management Maturity Model*	Modelo de maturidade para o gerenciamento de projetos.

MODELO DE MELHORES PRÁTICAS	ESCOPO DO MODELO
BSC – *Balanced Scorecard*	Metodologia de planejamento e gestão da estratégia.
Seis Sigma	Metodologia para melhoramento da qualidade de processos.
TOGAF	Modelo para o desenvolvimento e implementação de arquiteturas de negócio, aplicações e de tecnologia.
SAS 70 – *Statement on Auditing Standards for services organizations*	Regras de auditoria para empresas de serviços.

Fonte: Fernandes e Abreu (2008, p. 163-164).

No presente material, abordaremos dois dentre os modelos apresentados no quadro para exemplificar a aplicação das melhores práticas. São eles: o modelo COBIT e ITIL, que serão vistos nos tópicos a seguir.

5. COBIT

De acordo com Fernandes e Abreu (2008), o COBIT (*Control Objectives for Information and related Technology*) surgiu em 1994, apresentando, inicialmente, um conjunto de objetivos de controle, e, desde então, tem sofrido atualizações por meio da incorporação de padrões internacionais técnicos, regulatórios, profissionais e específicos para processos de TI.

A segunda edição (publicada em 1998) continha uma revisão dos objetivos de controle de alto nível e detalhados, além de agregar outras ferramentas e padrões para implementação. Já na sua terceira edição (publicada em 2000), o texto do COBIT foi publicado pelo IT Governance Institute, órgão criado pela ISACA (*Information Systems Audit and Control Association*), cujo objetivo é promover a melhoria do atendimento e a adoção dos princípios da Governança de TI.

Em 2005, surgiu a versão 4.0, que contemplava práticas e padrões com maior grau de maturidade e em conformidade com

as regulamentações, além de ampliar sua abrangência para um público mais heterogêneo, como gestores, especialistas, técnicos e auditores de TI.

Em 2007, foi apresentada outra atualização, a versão 4.1 (atual), que está focada em uma maior eficácia dos objetivos de controle e dos processos de verificação e divulgação de resultados. Dando sequência ao processo de atualizações, a ISACA anunciou o desenvolvimento da próxima versão da estrutura do COBIT e produtos de suporte, o COBIT 5.

Com base no uso prático do COBIT a mais de quinze anos por profissionais de TI, a nova versão 5.0 (de 2011) que tem como foco o atendimento às necessidades atuais e futuras das partes interessadas, se alinham com o pensamento atual de governança corporativa e práticas de gestão em TI**.**

A definição de Governança de TI presente no COBIT demonstra a importância da TI para as organizações, ou seja, a TI deve ser considerada parte integrante da estratégia corporativa. Partindo dessa realidade, os objetivos das práticas do COBIT devem contribuir para o sucesso na entrega de produtos e serviços de TI, sempre alinhada às exigências do negócio e focada mais no controle do que na execução propriamente dita.

O modelo do COBIT representa todos os processos encontrados nas funções da TI e deve ser entendível tanto para a operação quanto para os gerentes de negócios, uma vez que possibilita a criação de uma via comum entre as necessidades de execução (equipe operacional) e a visão que os executivos desejam ter para governar.

A base de sustentabilidade da Governança de TI, segundo o COBIT, pode ser representada por cinco áreas (Alinhamento estratégico, Agregação de valor, Gerenciamento de riscos, Gerenciamento de recursos e Medição de desempenho), cada uma delas com seu respectivo foco, conforme apresentado na Figura 2.

Figura 2 *Áreas-Foco da Governança de TI, na visão do COBIT*.

A seguir, descreveremos detalhadamente cada um desses focos.

1) **Alinhamento estratégico**: busca garantir a integração entre os planos de negócio e de TI, bem como a coesão das ideias das operações de TI e as da organização.
2) **Entrega de valor**: conforme descreve o COBIT (2007, p. 8):

   > [...] é a execução da proposta de valor de TI através do ciclo de entrega, garantindo que TI entrega os prometidos benefícios previstos na estratégia da organização, concentrando-se em otimizar custos e provendo o valor intrínseco de TI.

3) **Gerenciamento de riscos**: exige o conhecimento dos riscos por parte da alta direção da empresa, compreensão das tendências da empresa aos riscos e definição das responsabilidades para o processo de gestão de riscos na organização.
4) **Gerenciamento de recursos**: promove a melhoria dos investimentos e a correta gestão dos recursos críticos de TI (pessoas, aplicações, infraestrutura e informação), necessários para fornecimento dos subsídios indispensáveis à organização, para que esta cumpra os seus objetivos.

5) **Monitoração e *performance***: acompanha e monitora a implementação da estratégia, a conclusão do projeto, o uso de recursos, o desempenho de processos e a entrega de serviços, utilizando indicadores de desempenho, por exemplo, *balanced scorecards*, que transcrevem a estratégia em ações para alcançar metas mensuráveis.

A estrutura do COBIT é responsável por uma integração e institucionalização de boas práticas de planejamento e organização; aquisição e implementação; entrega e suporte; e monitoramento e avaliação de desempenho de TI. Assim que implantada integralmente, a Governança de TI permite um gerenciamento dos investimentos em tecnologia bem mais eficiente por parte da empresa, transformando-a em aumento de benefícios, oportunidades de negócio e vantagem competitiva no mercado.

Ainda conforme Fernandes e Abreu (2008), o COBIT utiliza-se de uma estrutura (*framework*) em que a ideia principal é a de atender às necessidades do controle organizacional relacionadas à Governança de TI, tendo como características principais o foco nos requisitos de negócio, a orientação para uma abordagem de processos, a utilização de mecanismos de controle e o direcionamento para análise das medições e indicadores de desempenho obtidos durante o decorrer do tempo.

Conforme o COBIT (2007), para uma empresa obter a informação que necessita para atingir suas metas de negócio, é preciso uma associação com suas metas de TI, bem como gerenciar e controlar os recursos de TI, utilizando um conjunto de processos bem-arranjados, a fim de garantir a entrega dos serviços de TI solicitados.

Ainda de acordo com o COBIT (2007), as informações desejadas devem obedecer a alguns parâmetros de controle ou requisitos de negócio, para que sua utilização traga retornos satisfatórios alinhados aos objetivos de negócio. Tais parâmetros são: eficiência, eficácia, confidencialidade, integridade, disponibilidade, conformidade com regulações e confiabilidade.

As informações necessárias para que uma organização atinja seus objetivos são fornecidas por meio de processos que utilizam recursos de TI, pessoas e infraestrutura para executar determinadas aplicações e rotinas que são responsáveis por processar as informações de negócio.

Existe um modelo padrão de referência, fornecido pelo COBIT, e uma linguagem comum, que permite que todos de uma determinada organização sejam capacitados para distinguir e gerenciar atividades de TI, utilizando como matriz o ciclo tradicional de melhoria contínua (planejar, construir, executar e monitorar). O COBIT (2007) identificou quatro domínios que retratam os agrupamentos existentes em uma determinada organização padrão de TI, que serão mostrados na Figura 3.

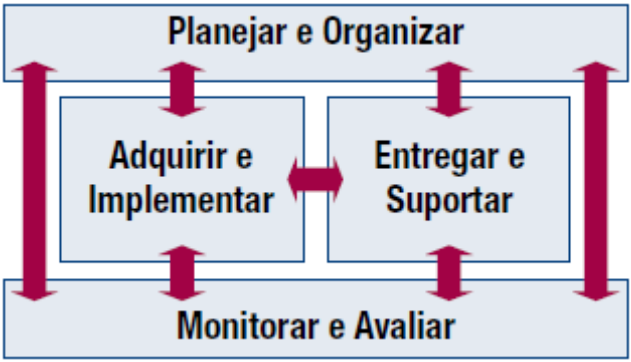


Figura 3 *Os quatro domínios inter-relacionados do COBIT*.

Cada domínio abrange um conjunto de 34 processos para garantir a completa gestão de TI. A seguir, definiremos cada um dos domínios e, no Quadro 2, a relação entre questões gerenciais e os processos envolvidos, ou seja, de um lado, são apresentadas questões estratégicas de nível gerencial, e, de outro, os processos envolvidos para alcançá-las ou respondê-las.

1) **Planejar e organizar**: domínio que abrange o planejamento e a organização, buscando identificar as melhores maneiras de contribuição por parte da TI para o alcance dos objetivos do negócio.

2) **Adquirir e implementar**: domínio responsável pela aquisição e implementação das soluções identificadas pela estratégia de TI. Também trata do acompanhamento de mudanças, para que estas não afetem os resultados, ou seja, os objetivos do negócio.
3) **Entregar e suportar**: domínio dedicado à entrega e ao suporte dos serviços requisitados.
4) **Monitorar e avaliar**: domínio responsável por monitorar e avaliar os processos de TI durante seu ciclo de execução, abordando o gerenciamento de desempenho, monitoramento do controle interno e a governança.

Quadro 2 Questões e processos dos domínios do COBIT.

	QUESTÕES GERENCIAIS	PROCESSOS DE TI
Planejar e Organizar	As estratégias de TI e de negócios estão alinhadas? A empresa está obtendo um ótimo uso dos seus recursos? Todos na organização entendem os objetivos de TI? Os riscos de TI são entendidos e estão sendo gerenciados? A qualidade dos sistemas de TI é adequada às necessidades de negócios?	**PO1** Definir um plano estratégico de TI **PO2** Definir a arquitetura da informação **PO3** Determinar as diretrizes de tecnologia **PO4** Definir os processos, a organização e os relacionamentos de TI **PO5** Gerenciar o investimento de TI **PO6** Comunicar metas e diretrizes gerenciais **PO7** Gerenciar os recursos humanos de TI **PO8** Gerenciar a qualidade **PO9** Avaliar e gerenciar os riscos de TI **PO10** Gerenciar projetos
Adquirir e Implementar	Os novos projetos serão entregues no tempo e com o orçamento previstos? Os novos sistemas ocorreram apropriadamente quando implementados? As alterações ocorrerão sem afetar as operações de negócios atuais?	**AI1** Identificar soluções automatizadas **AI2** Adquirir e manter *software* aplicativo **AI3** Adquirir e manter infraestrutura de tecnologia **AI4** Habilitar operação e uso **AI5** Adquirir recursos de TI **AI6** Gerenciar mudanças **AI7** Instalar e homologar soluções e mudanças

	QUESTÕES GERENCIAIS	PROCESSOS DE TI
Entregar e Suportar	Os serviços de TI estão sendo entregues de acordo com as prioridades de negócios? Os custos de TI estão otimizados? A força de trabalho está habilitada para utilizar os sistemas de TI de maneira produtiva e segura? Os aspectos de confidencialidade, integridade e disponibilidade estão sendo contemplados para garantir a segurança da informação?	**DS1** Definir e gerenciar níveis de serviços **DS2** Gerenciar serviços terceirizados **DS3** Gerenciar o desempenho e a capacidade **DS4** Assegurar a continuidade dos serviços **DS5** Garantir a segurança dos sistemas **DS6** Identificar e alocar custos **DS7** Educar e treinar os usuários **DS8** Gerenciar a central de serviço e os incidentes **DS9** Gerenciar a configuração **DS10** Gerenciar problemas **DS11** Gerenciar os dados **DS12** Gerenciar o ambiente físico **DS13** Gerenciar as operações
Monitorar e Avaliar	A *performance* de TI é mensurada para detectar problemas antes que seja muito tarde? O gerenciamento assegura que os controles internos sejam efetivos e eficientes? O desempenho da TI pode ser associado aos objetivos de negócio? Existem controles adequados para garantir confidencialidade, integridade e disponibilidade das informações?	**ME1** Monitorar e avaliar o desempenho de TI **ME2** Monitorar e avaliar os controles internos **ME3** Assegurar a conformidade com requisitos externos **ME4** Prover Governança de TI

Fonte: adaptado de Fernandes e Abreu (2008, p. 179).

De acordo com Fernandes e Abreu (2008, p. 181):

> [...] o COBIT define como controle o conjunto de políticas, procedimentos, práticas e estruturas organizacionais desenvolvidas para dar uma garantia razoável de que os objetivos de negócio serão atingidos e de que os eventos indesejáveis serão prevenidos ou mesmo detectados e corrigidos.

O processo de controle é bastante simples: as informações de controle extraídas de cada processo de TI são analisadas e comparadas com os objetivos de controle, e as ações necessárias são tomadas como forma de prevenção ou correção, gerando, assim, uma considerável melhoria no processo.

Uma das maiores dificuldades para as empresas é a visualização do nível de profundidade que deve ser adotado pelos mecanismos de controle e medições de desempenho. As organizações devem realizar uma medição que seja relativa à situação atual, focando nos aspectos para os quais melhorias se fazem necessárias, e realizar uma monitoração dessas ações de forma sistemática. Por fim, deve-se analisar a relação custo/benefício do controle. Obter uma visão objetiva do nível de desempenho da própria organização não é uma tarefa tão simples. Dentre as dúvidas que surgem, primeiramente, deve-se identificar o que tem de ser avaliado e de que maneira será feito.

O COBIT (2007, p. 19) lida com essas questões fornecendo publicações que contenham:

- Modelos de maturidade que permitem fazer comparações e identificar os necessários aprimoramentos de capacidades.
- Objetivos de desempenho e métricas para os processos de TI, demonstrando como os processos atingem os objetivos de negócios e de TI e são utilizados para medir o desempenho dos processos internos baseados nos princípios do *balanced scorecard*.
- Objetivo de atividades para habilitar o efetivo desempenho do processo.

Modelos de maturidade

O modelo de maturidade para o gerenciamento e controle dos processos de TI é baseado num método de avaliar a organização, permitindo que ela seja pontuada de um nível de maturidade não existente (0) a otimizado (5).

1) **Nível 0 – Inexistente**: não existem processos de gestão.
2) **Nível 1 – Inicial/*Ad hoc***: os processos de gestão são casuais e desorganizados.
3) **Nível 2 – Repetitivo, porém intuitivo**: os processos tornam-se regulares, porém dependem exclusivamente do conhecimento dos indivíduos. Tal dependência pode acarretar erros.

4) **Nível 3 – Processo definido**: os processos são padronizados, documentados e, por fim, comunicados.
5) **Nível 4 – Gerenciado e mensurável**: os processos são monitorados e medidos pela gerência, a fim de verificar se estão em conformidade com os procedimentos. Caso os resultados não sejam o esperado, ações são tomadas.
6) **Nível 5 – Otimizado**: são aplicadas as boas práticas evidenciadas em resultados de melhorias contínuas. Por fim, a TI passa a ser considerada uma ferramenta de interação, atuando na automatização do fluxo e trabalho.

Os modelos de maturidade anteriormente apresentados, quando aplicados, podem garantir à gerência a capacidade de:

1) identificar o cenário atual da organização;
2) realizar um comparativo do cenário atual com as demais organizações em destaque no segmento;
3) realizar um comparativo com os mais elevados padrões internacionais;
4) determinar e monitorar na íntegra as melhorias dos processos, buscando alinhá-los à estratégia da organização.

Metas e medições de desempenho

As metas e medições de desempenho são definidas no COBIT (2007) em três níveis:

1) O que os negócios esperam de TI (**metas de TI**).
2) O que os processos de TI precisam entregar para suportar os seus próprios objetivos (**metas de processo**).
3) O que precisa acontecer dentro do processo para que se atinja o desempenho desejado (**metas de atividades**).

Para tal, o COBIT (2007) utiliza-se de dois tipos de indicadores, denominados a seguir:

1) **Medições de resultados**: definem as medições que informam à alta direção da empresa se um processo de TI atingiu os objetivos de negócio.

2) **Indicadores de desempenho**: definem as medições que informam à alta direção da empresa o quanto os processos de TI são bem executados, viabilizando o atendimento dos objetivos de negócio.

Aplicabilidade do modelo COBIT

Dentre as várias possibilidades de aplicação do modelo COBIT em uma organização, podemos ressaltar:

1) **Avaliação dos processos de TI**: em razão da grande abrangência do COBIT e seu alto nível de padronização, torna-se possível sua utilização como um *checklist*, ou seja, pode ser utilizado como uma ferramenta de avaliação dos pontos positivos e negativos dos processos, servindo como base para a elaboração de ações de melhoria.
2) **Auditoria dos riscos operacionais de TI**: a avaliação dos processos pode se dar em conjunto ou isoladamente, e as suas inconsistências em relação aos padrões analisadas, em relação aos riscos que podem representar para o negócio da empresa, em termos de sua probabilidade de ocorrência e, por fim, da severidade do impacto [*sic*].
3) **Implementação modular da Governança de TI**: as práticas e os padrões relativos a áreas e processos específicos podem ser mapeados para os processos do modelo, a fim de criar uma estrutura hierárquica de processos de gestão, aproveitando-se de práticas e processos já existentes.
4) **Realização de *benchmarking***: uma vez existindo modelos de maturidade para cada processo de TI, torna-se possível que uma organização seja capaz de criar uma estratégia com base na sua situação atual em termos de Governança de TI, utilizando como parâmetros de comparação os dados de outras empresas ou padrões internacionais de mercado e estabelecendo suas próprias metas de melhoria contínua e de crescimento.
5) **Qualificação de fornecedores de TI**: igualmente ao mercado de desenvolvimento de *software*, os modelos de maturidade do COBIT podem ser utilizados como qualifi-

cadores na contratação de serviços de TI, como também no estabelecimento de níveis de serviço dentro de uma organização. Uma grande vantagem da utilização desses modelos é a padronização, isto é, a utilização dos mesmos critérios para avaliar processos em diversas organizações.

O COBIT pode ser implantado tanto em pequenas organizações quanto em grandes empresas de TI, uma vez que esteja coerente com seus objetivos de negócios e com as suas estratégias de TI. Em relação ao público-alvo interno de uma organização, o COBIT aplica-se aos usuários por meio de focos distintos (FERNANDES; ABREU, 2008, p. 188):

1. **Gestão executiva**: orienta como obter retorno sobre os investimentos em TI, auxiliando a balanceá-los com os riscos inerentes ao ambiente de TI.
2. **Gestão do negócio**: auxilia a obter maiores garantias sobre o gerenciamento dos serviços de TI, prestados por colaboradores internos ou terceirizados.
3. **Gestão de TI**: auxilia a prover os serviços de TI adequados que suportem a estratégia do negócio, de forma controlada e gerenciada.
4. **Auditores**: fornece informações para suas conclusões e orientação para a gestão dos controles internos.

Certificações relacionadas

As certificações do COBIT são divididas em dois programas avançados, patrocinados pelo ISACA, conforme segue:

- **CISA (*Certified Information Systems Auditor*)**: em português, "Certificação de Auditores de Sistemas de Informação", certifica o grau de conhecimento e a excelência do candidato em relação às disciplinas de auditoria, controle e segurança de TI. Trata-se de um dos exames de certificação mais eficaz do mercado.
- **CISM (*Certified Information Security Manager*)**: em português, "Certificação de Gerente de Segurança da Infor-

mação", destina-se a profissionais especialistas da área de segurança da informação, desde o planejamento até a execução das atividades pertinentes. Abrange os cinco principais conceitos sobre o tema: governança de segurança da informação, gestão de programas de segurança da informação, gestão de riscos, gestão da segurança da informação e gestão de respostas a eventos.

Para os profissionais que buscam uma visão mais geral dos conceitos e processos do COBIT, bem como da sua implantação prática, o ISACA oferece outro modelo de certificação: o COBIT Foundation.

A estrutura do COBIT favorece a compreensão dos processos de TI, fornecendo um excelente guia para sua aplicação ou melhoria nas organizações e subsídios para análise da maturidade atual dos processos existentes. Resumindo, a utilização do COBIT pelas organizações pode estabelecer bases mais sólidas para um retorno sobre os investimentos em TI.

No próximo tópico, será apresentado um dos principais modelos de melhores práticas: o modelo ITIL.

6. ITIL

A necessidade de padronização dos processos na área de TI, como também a busca da melhoria dos níveis de qualidade dos serviços prestados ao governo britânico, foram os fatores que alavancaram o surgimento da Information Technology Infrastructure Library (ITIL), no final da década de 1980.

Após passar por revisões e adequações, em 2007, foi lançada a Versão 3 da ITIL, que propõe a organização dos processos de gerenciamento de serviços por meio de uma estrutura do ciclo de vida de serviço. Também se destaca nessa última versão o conceito de integração da TI ao negócio e a possibilidade de convergência com os demais padrões de gestão e governança, como COBIT, PMBOK, CMMI, entre outros.

Podemos definir a ITIL como uma biblioteca das melhores práticas utilizadas na gestão dos serviços de TI que foram desenvolvidas por meio do trabalho e pesquisa dos profissionais dessa área durante algumas décadas, elegendo-a, assim, como um padrão mundialmente seguido.

O principal objetivo da ITIL é a elaboração de tais práticas (implantadas, testadas e aprovadas pelas organizações), as quais podem ser utilizadas por empresas que já apresentam determinada maturidade em seus processos e desejam conceber melhorias, como também para criação de novos processos.

A seguir, apresentaremos os principais componentes da ITIL:

- **Núcleo da ITIL**: orientações das melhores práticas cabíveis a todas as organizações prestadoras de serviços para um negócio.
- **Orientação complementar à ITIL**: publicações complementares que buscam o aprimoramento da implementação e a utilização das práticas do núcleo, por exemplo, para setores empresariais distintos.

O Quadro 3 apresenta os grupos de processos da ITIL V3 (Versão 3), que se encontram distribuídos entre cinco estágios. Os processos podem ser compreendidos como procedimentos necessários para gerenciar a infraestrutura de TI de maneira eficiente e eficaz, visando garantir os níveis de serviço, tanto internos quanto externos, acordados com os clientes.

Quadro 3 Processos e funções da ITIL V3.

PUBLICAÇÕES	PROCESSOS	FUNÇÕES
Estratégia de Serviço	Gerenciamento Financeiro de TI. Gerenciamento de *Portfolio* de Serviços. Gerenciamento da Demanda.	

PUBLICAÇÕES	PROCESSOS	FUNÇÕES
Desenho de Serviço	Gerenciamento do Catálogo de Serviços. Gerenciamento do Nível de Serviço. Gerenciamento da Capacidade. Gerenciamento da Disponibilidade. Gerenciamento da Continuidade de Serviço. Gerenciamento de Segurança da Informação. Gerenciamento de Fornecedor.	
Transcrição de Serviço	Gerenciamento de Mudança. Gerenciamento da Configuração e de Ativo de Serviço. Gerenciamento da Liberação e Implantação. Validação e Teste de Serviço. Avaliação. Gerenciamento do Conhecimento.	
Operação de Serviço	Gerenciamento de Evento. Gerenciamento de Incidente. Cumprimento de Requisição. Gerenciamento de Problema. Gerenciamento de Acesso.	Central de Serviço. Gerenciamento Técnico. Gerenciamento das Operações de TI. Gerenciamento de Aplicativo.
Melhoria de Serviço Continuada	Relatório de Serviço. Medição de Serviço.	

Fonte: Fernandes e Abreu (2008, p. 275).

Uma vez apresentados os estágios do ciclo de vida de serviço da ITIL V3, detalharemos, a seguir, seus principais aspectos: estratégia de serviço, desenho de serviço, transição de serviço, operação de serviço e melhoria de serviço continuada.

Estratégia de Serviço

A estratégia de serviço apresenta os princípios fundamentais que conduzem o gerenciamento de serviços, demonstrando às empresas como podem transformá-lo em um ativo de sucesso, além de fornecer orientações para que estas cresçam a longo prazo. Nesse cenário, surgem algumas questões acerca da implementação do gerenciamento de serviços, por exemplo, que tipo de serviços e a quem serão oferecidos, como se destacar perante os concorrentes, como definir a qualidade dos serviços e como melhorá-los, entre outras.

O desenvolvimento da estratégia de serviço pode se dar por meio de quatro fases bem definidas:

1) **Definição do mercado**: trata da definição de relação entre a estratégia e o serviço, bem como do entendimento do cliente.
2) **Desenvolvimento de ofertas**: uma vez definido o mercado-alvo, trata do desenvolvimento de serviços com base na proposta de valor que podem agregar aos ativos dos clientes.
3) **Desenvolvimento de ativos estratégicos**: se um provedor aumentar o potencial de um serviço, ocorre o mesmo com o potencial de desempenho dos ativos dos clientes, desencadeando, também, um aumento na demanda pelo serviço. O resultado é a redução da ociosidade do provedor de serviços.
4) **Preparação para execução**: basicamente, trata do estudo estratégico das ofertas e da definição dos objetivos.

Observando o Quadro 3, podemos notar os processos de Gerenciamento de Serviços que integram o estágio da Estratégia de Serviço. A seguir, definiremos cada um deles:

- **Gestão Financeira**: trata da gestão do ciclo financeiro do Portfólio de Serviços de Tecnologia da Informação, fornecendo equilíbrio nas receitas, com o objetivo de proporcionar aos serviços condições para que sejam executados.

Um dos indicadores mais utilizados dentro do processo de gerenciamento financeiro é conhecido como Retorno sobre o Investimento, ou simplesmente **ROI**. Trata-se de um índice de medição utilizado para justificar o investimento em serviços, demonstrando, por fim, o retorno obtido.

- **Gestão de Portfólio de Serviços**: baseia-se na gestão dos investimentos em gerenciamento de serviços, com o objetivo específico de agregar valor à organização.
- **Gestão de Demanda**: trata da gestão dos ciclos de produção dos serviços, para os casos de consumo de demanda e dos ciclos de consumo dos serviços, para os casos de aumento na geração de demanda.

Desenho de Serviço

Conforme Fernandes e Abreu (2008, p. 281):

> A ITIL V3 define o Desenho de Serviço como "o desenho de serviços de TI apropriados e inovadores, incluindo suas arquiteturas, processos, políticas e documentação, para atender os requisitos do negócio atuais e futuros".

Essa publicação tem como objetivo o desenho e a elaboração dos serviços de TI, que, por sua vez, devem garantir a realização da estratégia montada anteriormente. A publicação ocorre da seguinte maneira:

- Definir como deve ser tratado o desenho de um novo serviço ou a alteração de um serviço existente. Ambos devem ser trabalhados como projeto de solução completa e sempre alinhados com a estratégia estabelecida pela organização.
- Abordar, na sequência, o desenho de sistemas e ferramentas de gerenciamento de serviços que serão utilizados pelos serviços em todas as etapas do ciclo de vida, bem como o desenho de arquiteturas tecnológicas e sistemas de gestão, e descrever, também, o desenho dos

processos de TI e de Gerenciamento de Serviços, nos quais são atribuídas habilidades e responsabilidades que visam à operação, ao apoio e à manutenção dos serviços.

- Tratar do aspecto de desenho de métricas e métodos de medição, normalmente da qualidade do processo de desenho de serviço, observando indicadores, como o progresso, a conformidade com o escopo, os requisitos de regulação, entre outros.

No Quadro 3, podemos observar os sete processos de Gerenciamento de Serviços que integram o estágio de Desenho de Serviço. A seguir, definiremos cada um deles:

1) **Gerenciamento do Catálogo de Serviços**: administra um repositório centralizado de informações atualizadas sobre todos os serviços que se encontram em produção, como também daqueles em fase de preparação para entrada em operação. O Catálogo de Serviços normalmente se apresenta subdividido em Catálogo de Serviços de Negócio e Catálogo de Serviços Técnicos, garantindo, dessa maneira, uma maior homogeneidade na gestão dos processos.
2) **Gerenciamento do n**ível de **serviço**: esse processo trabalha na gestão da manutenção e implementação de melhorias da qualidade dos serviços de TI, como também é de sua responsabilidade a elaboração e a atualização do Plano de Melhoria dos Serviços.
3) **Gerenciamento da capacidade**: monitora a capacidade da infraestrutura de TI em atender as demandas do negócio e aperfeiçoa-a quando necessário.
4) **Gerenciamento e disponibilidade**: busca garantir que os serviços de TI mantenham os níveis de confiabilidade e disponibilidade exigidos pelo negócio.
5) **Gerenciamento da continuidade de serviço**: busca garantir que os recursos e os serviços de TI sejam recuperados dentro do período de tempo predeterminado pelo negócio.

6) **Gerenciamento de segurança da informação**: envolve alguns processos relacionados a confiabilidade, disponibilidade e integridade dos dados, bem como visa garantir a segurança dos componentes de *software* e *hardware*.
7) **Gerenciamento de fornecedores**: realiza a gestão dos fornecedores e contratos.

Um dos fatores que devem ser observados por ocasião da implementação do Desenho de Serviço em uma organização é a necessidade de definir claramente uma matriz de responsabilidades, ou seja, estabelecer quais serão as atribuições de cada função, por exemplo, Gestor de Catálogo de Serviços, Gestor de Disponibilidade, Gestor de Segurança da Informação, entre outras.

Transição de Serviço

O estágio de Transição de Serviço visa inserir um serviço recém-modelado no estágio de Desenho de Serviço, em um ambiente de produção, sem que seja necessário providenciar paralisação de suas operações, agregando valor à organização, tanto pela disponibilidade de oferta de novos serviços quanto pela demonstração da sua capacidade de gestão de mudanças de seus serviços de uma maneira eficiente.

Ainda no Quadro 3, podemos observar os seis processos de Gerenciamento de Serviços que integram o estágio de Transição de Serviço. A seguir, apresentaremos cada um deles:

1) **Gerenciamento de mudança**: seu objetivo é garantir que as mudanças efetuadas em ambiente operacional obedeçam a uma padronização e, dessa maneira, reduzam qualquer tipo de impacto e melhorem a rotina operacional da organização.
2) **Gerenciamento da configuração e de ativo de serviço**: envolve a identificação, o controle e o registro de ativos de serviço e os itens de configuração, como, por exemplo, versões de *software*. Além disso, monitora a segurança da integridade dos ativos e itens de configuração contra mudanças não autorizadas.

3) **Gerenciamento de liberação e implementação**: trabalha na gestão das mudanças devidamente autorizadas em um serviço de TI, produzindo componentes de saída alinhados com os requisitos do cliente, que deverão ser implementados em seu ambiente de produção.
4) **Validação e teste de serviço**: esse processo atua no controle de qualidade de uma liberação, ou seja, um serviço validado e testado deverá estar em conformidade com os requisitos e atender as necessidades para as quais foi desenhado.
5) **Avaliação**: busca o desenvolvimento de mecanismos padronizados para medição do desempenho de mudanças em um ambiente de infraestrutura de TI e serviços em produção, comparando-os com as metas estabelecidas e apontando quaisquer desvios, caso eles existam.
6) **Gerenciamento do conhecimento**: busca garantir a entrega da informação correta no local certo e para a pessoa capaz de realizar as ações necessárias.

O estágio de Transição de Serviço também agrega algumas funções na matriz de responsabilidades, por exemplo, Gestor de Mudanças, Gerente de Avaliação, entre outros.

Operação de Serviço

O estágio de Operação de Serviço requer uma atenção redobrada, em virtude de ser considerado de alta criticidade dentro do ciclo de vida do serviço, pois, caso apresente falha na sua condução, a disponibilidade do serviço poderá ser comprometida.

O objetivo da Operação de Serviço é a coordenação e a execução das atividades de entrega e suporte aos serviços, sempre em conformidade com os acordos estabelecidos com os clientes.

Como se pode observar no Quadro 3, há cinco processos de Gerenciamento de Serviços que integram o estágio de Operação de Serviço. A seguir, detalharemos cada um deles:

1) **Gerenciamento de evento**: atua no gerenciamento e monitoramento dos eventos que ocorrem na infraestru-

tura de TI, a fim de atestar a normalidade da operação. Se, diferentemente disso, anormalidades forem identificadas, o processo de gerenciamento de evento é responsável pelo escalonamento para solução técnica ou para atuação hierárquica.

2) **Gerenciamento de incidente**: tem como objetivo o reestabelecimento da operação de um serviço o mais rápido possível, buscando minimizar os impactos para o negócio.
3) **Cumprimento de requisição**: trata das requisições dos usuários (solicitação de serviço e/ou informação) que não foram geradas por um incidente.
4) **Gerenciamento de problema**: busca mitigar os impactos causados por incidentes ou falhas na infraestrutura de TI, tratando (proativa ou reativamente) da prevenção para que tais incidentes não voltem a ocorrer.
5) **Gerenciamento de acesso**: atua no controle do acesso de usuários a recursos e serviços, permitindo acesso somente àqueles usuários que foram previamente autorizados, bem como bloqueando o acesso aos demais.

De acordo com Fernandes e Abreu (2008, p. 292), a ITIL V3 define "função" como "um conceito lógico referente a pessoas e medidas automatizadas que executam um determinado processo, atividade, ou uma comunicação entre eles". A seguir, serão apresentadas as quatro funções que fazem parte do estágio de Operação de Serviço:

1) **Central de Serviço**: também conhecido como "*Service Desk*", tem a função de prover respostas rápidas às requisições dos usuários, podendo apresentar-se de forma centralizada, virtual ou local, como Central de Atendimento, ou *Call Center*, (atendimento de grande volume de chamadas telefônicas) e *Help Desk* (resolução de incidentes com brevidade).
2) **Gerenciamento t**écnico: trata-se de uma função voltada para as áreas ou equipes que detêm conhecimento técnico e experiência para dar suporte à operação.

3) **Gerenciamento das operações de TI**: trata-se de uma função voltada para as áreas ou equipes que efetivamente executam as atividades cotidianas da operação.
4) **Gerenciamento de aplicativo**: realiza a gestão dos aplicativos durante o seu ciclo de vida. No caso dos aplicativos de *softwares* relacionados à implementação de serviços em TI, inclui, também, o gerenciamento das atividades de desenvolvimento, desde o levantamento de requisitos até a realização de testes, e atividades de gerenciamento, da implementação ao suporte e otimização.

Melhoria de Serviço Continuada

O estágio de Melhoria de Serviço Continuada busca colocar em prática o constante alinhamento e integração dos serviços de TI com as necessidades do negócio. Isso se dá por meio da implementação de práticas de melhoria para o suporte aos processos de negócio.

Resumindo, esse estágio se propõe a desenvolver ou planejar melhorias contínuas dos processos. Para verificação dos resultados dos benefícios da aplicação, pode-se utilizar como métrica, por exemplo, a quantidade de falhas durante a realização das melhorias, como também podem ser medidas pelos indicadores como retorno sobre o investimento e valor sobre o investimento.

Ao voltar para o Quadro 3, podemos observar os processos de Gerenciamento de Serviços que integram o estágio de Melhoria de Serviço Continuada, conforme detalhamento a seguir:

- **Relatório de Serviço**: trata da elaboração de relatórios baseados em dados coletados durante a entrega do serviço.
- **Medição de Serviço**: realiza a divulgação de informações sobre o serviço a partir de uma visão macro orientada à integração com o negócio.

Várias modalidades no quesito prestação de serviços são parecidas com a ITIL, tanto local quanto remotamente, e necessitam

de uma abordagem de gestão. O modelo ITIL vem sendo bastante utilizado em projetos e operações continuadas que envolvem itens de infraestrutura, principalmente por causa da grande prioridade que vem sendo dada aos aspectos tecnológicos.

O modelo ITIL pode ser aplicado a serviços específicos de gerenciamento de serviços operacionais, tais como manutenções, operações de indústria de *software*, *outsourcing* de desenvolvimento, entre outras. Com a chegada do ITIL V3, o modelo ganhou muitas possibilidades de aplicação nas organizações, desde empresas pequenas até as grandes corporações.

A utilização das informações provenientes da análise da base de conhecimento da organização certamente possuía como resultado um plano de melhoria dos serviços, no qual o foco e o valor eram adicionados ao negócio.

Deve-se também atentar para o estágio de Transição de Serviço, ou seja, para a fase que precede o lançamento perante clientes e/ou usuários dos serviços projetados e executados. Nesse momento, os serviços precisam ser testados de todas as maneiras, para avaliar-se a capacidade de satisfazer os níveis exigidos pelo negócio.

Para a implementação do modelo, recomenda-se que seja feita de forma gradativa, ou seja, parta de um princípio reduzido de operações como base e promova lançamentos ou atualizações de maneira sucessiva para o restante das operações, dando o devido respeito às interdependências existentes entre os processos de gestão e os requisitos de disponibilidade e continuidade dos serviços.

Outro ponto importante são as questões relacionadas à estrutura organizacional e à tecnologia que suporta os serviços, fazendo que os pontos fortes sejam aproveitados da melhor maneira possível, deixando em aberto para mudanças que gerem o menor impacto possível no que diz respeito à disponibilidade dos recursos.

Como nem todo modelo é perfeito, a ITIL também pode precisar de algumas adaptações, em função das características de cada organização de TI, dos serviços previstos em seu catálogo e dos níveis de serviço exigidos. Analisando dessa forma, uma organização deve sempre considerar os desafios, os fatores críticos de sucesso e os riscos à sua estrutura.

Como a maioria dos outros modelos, a ITIL V3 apresenta seu próprio formato para as qualificações ou certificações dos candidatos. Seu formato baseia-se em um sistema de créditos cumulativos, agrupados em três níveis de certificação, conforme veremos a seguir:

1) **Nível básico** (***foundations***): aplica-se a candidatos com habilidades básicas, ou seja, que conheçam os principais conceitos, terminologias e processos que abrangem a ITIL V3. Equivale a dois créditos no programa de certificação.
2) **Nível intermediário**: aplica-se a candidatos com maior bagagem de conhecimento ou grau de especialização. Essa certificação pode ser conquistada por meio de dois caminhos distintos: a corrente do ciclo de vida ou a corrente de capacitação. Equivalem sucessivamente a três e quatro créditos no programa de certificação.
3) **Nível avançado**: aplica-se a candidatos e profissionais que possuem nível avançado de conhecimento acerca do assunto. Essa certificação inclui o curso de Gerenciamento por intermédio do Ciclo de Vida, em que é apresentada uma visão completa sobre o ciclo de vida no contexto da gestão de serviços em TI. Equivale a cinco créditos no programa de certificação.

Para que o candidato seja considerado um certificado ITIL, é necessária a realização de um exame de qualificação profissional, ministrado por um dos institutos oficiais a seguir:

- APM Group (APMG): empresa global autorizada a fornecer serviços de validação e certificação.
- EXIN (Examination Institute for Information Science in the Netherlands).

7. COMPARATIVO ENTRE OS MODELOS

Agora que você tem uma visão geral sobre o modelo, torna-se mais fácil a compreensão da sua importância e aplicabilidade. Além disso, as boas práticas descritas pela ITIL são compatíveis com inúmeros perfis de prestação de serviços de TI que buscam uma boa forma de gestão.

A ITIL V3 possibilita a implementação tanto em grandes organizações, com níveis avançados de maturidade em seus processos, quanto em organizações menores, que se encontram no estágio de iniciação pela busca da qualidade de serviços.

Nesse momento, cabe uma breve apresentação de como os modelos de melhores práticas se relacionam. O objetivo da elaboração dessa comparação entre as práticas é dar suporte a questões relacionadas à escolha do modelo e em que circunstâncias devem ser aplicados. Primeiramente, por definição, tomaremos o modelo COBIT como padrão para comparação com os demais modelos.

Segundo Fernandes e Abreu (2008, p. 415), "o COBIT, de todos os modelos de melhores práticas, nos parece o mais abrangente em termos de atendimento à gestão de TI".

O Quadro 4 apresenta o agrupamento dos modelos de melhores práticas conforme seus objetivos, visando a uma comparação com o COBIT.

Quadro 4 Agrupamento de modelos de melhores práticas.

Modelos Relacionados a Projetos	Modelos Relacionados a Serviços de TI	Modelos Relacionados a Terceiros	Modelos Relacionados a Desempenho e Melhoria	Modelos Relacionados a Segurança da Informação
CMMI	ITIL/ISO 20000	eSCM-SP	BSC	ISO 27001
Modelos PMI	MOF	eSCM-CL	Seis Sigma	ISO 27002
PRINCE 2	HP ITSM	SAS 70	Val IT	ISO 15408
RUP				

Modelos Relacionados a Projetos	Modelos Relacionados a Serviços de TI	Modelos Relacionados a Terceiros	Modelos Relacionados a Desempenho e Melhoria	Modelos Relacionados a Segurança da Informação
MSF				
ISO 12207				
ISO 9001				
ISO 9126				

Fonte: Fernandes e Abreu (2008, p. 415).

No Quadro 5, será apresentado o mapa de cobertura entre o COBIT Versão 4.0 e o modelo de melhores práticas ITIL V2. Para a coluna de cobertura ITIL no mapa a seguir, foi adotada a legenda: (E) Excede, (C) Cobertura Completa, (A) Vários aspectos abordados e (N/A) Não se aplica.

Quadro 5 Mapa de cobertura COBIT x ITIL.

	COBIT 4.0	COBERTURA ITIL
PO1	Definir um plano estratégico para TI.	A
PO2	Definir a arquitetura da informação.	N/A
PO3	Definir a direção tecnológica.	N/A
PO4	Definir a organização de TI, os seus processos e relacionamentos.	A
PO5	Gerenciar o investimento em TI.	A
PO6	Comunicar objetivos e direcionamentos gerenciais.	N/A
PO7	Gerenciar os recursos humanos.	A
PO8	Gerenciar a qualidade.	N/A
PO9	Avaliar e gerenciar riscos de TI.	A
PO10	Gerenciar projetos.	A
AI1	Identificar soluções automatizadas.	A
AI2	Adquirir e manter *software* aplicativo.	A
AI3	Adquirir e manter infraestrutura tecnológica.	A
AI4	Viabilizar operação e utilização.	A
AI5	Adquirir recursos de TI.	N/A
AI6	Gerenciar mudanças.	A
AI7	Instalar e aprovar soluções e mudanças.	A

	COBIT 4.0	COBERTURA ITIL
DS1	Definir e gerenciar níveis de serviço.	C
DS2	Gerenciar serviços terceirizados.	A
DS3	Gerenciar desempenho e capacidade.	C
DS4	Garantir a continuidade dos serviços.	A
DS5	Garantir a segurança dos sistemas.	A
DS6	Identificar e alocar custos.	C
DS7	Educar e treinar usuários.	N/A
DS8	Gerenciar central de serviços e incidentes.	C
DS9	Gerenciar a configuração.	C
DS10	Gerenciar problemas.	C
DS11	Gerenciar dados.	A
DS12	Gerenciar o ambiente físico.	N/A
DS13	Gerenciar operações.	N/A
ME1	Monitorar e avaliar o desempenho da TI.	N/A
ME2	Monitorar e avaliar os controles internos.	N/A
ME3	Assegurar conformidade com requisitos externos.	N/A
ME4	Fornecer governança para a TI.	N/A

Fonte: adaptado de Fernandes e Abreu (2008, p. 416).

Após este breve estudo comparativo entre os modelos de melhores práticas COBIT e ITIL, nada melhor do que visualizarmos efetivamente suas aplicabilidades.

Assim, aconselhamos a leitura integral dos dois estudos de caso de implementação de Governança de TI apresentados na obra *Implantando a governança de TI*: *da estratégia à gestão dos processos e serviços*, de Aguinaldo Aragon Fernandes e Vladimir Ferraz de Abreu, indicada nas *Referências Bibliográficas*.

8. QUESTÕES AUTOAVALIATIVAS

Confira, a seguir, as questões propostas para verificar o seu desempenho no estudo desta unidade:

1) Defina com suas próprias palavras "Governança de TI" e quais as suas implicações para as organizações de TI.

2) Qual é o objetivo do COBIT?

3) Qual é o melhor caminho e o mais rápido para vender COBIT para os gerentes de TI?

4) O modelo de melhores práticas COBIT é superior aos outros modelos de controle aceitos?

5) Dentre os quatro domínios identificados pelo COBIT que retratam os agrupamentos existentes em uma determinada organização padrão de TI, identifique e explique os processos relacionados ao domínio Entregar e Suportar.

6) O COBIT apresenta três dimensões de maturidade. Quais são os seus significados?

7) Como você executaria uma avaliação de maturidade baseada no modelo COBIT?

8) Caso as avaliações de maturidade não sejam medidas com exatidão, é realmente possível aferir os níveis de maturidade de uma organização?

9) Podemos definir a ITIL como uma biblioteca das melhores práticas utilizadas na gestão dos serviços de TI. Nesse cenário, quais os principais componentes da ITIL?

10) Na Central de Serviços, um usuário reclama, com razão, que o servidor de arquivos de seu departamento está fora do ar. O processo ITIL V2, que assegura o restabelecimento mais breve possível do serviço relacionado, é o gerenciamento de:

a) ( ) Mudanças
b) ( ) Problemas
c) ( ) Incidentes
d) ( ) Nível de serviço
e) ( ) Disponibilidade

Justifique sua resposta.

11) Qual a importância das definições apresentadas pela matriz de responsabilidades mostrada no modelo ITIL, como, por exemplo, a Gestão de Segurança da Informação?

12) O que é certificação ITIL e quais as disponíveis no mercado?

13) Em uma organização que tenha muitos projetos integrados de TI, qual o modelo de melhores práticas que você indicaria o uso?

14) Uma empresa que utiliza o COBIT 4.0 como modelo de melhores práticas para Governança de TI estabeleceu como meta, até o final do ano vigente, executar um Plano de Ação com o objetivo de elevar o nível de maturidade de seus processos prioritários de 2 para 3. Isso significa que:

a) ( ) seus processos seguem um padrão de regularidade e deseja-se atingir um nível em que estes sejam documentados e comunicados.
b) ( ) seus processos seguem um padrão de regularidade e deseja-se atingir um nível em que estes sejam monitorados e medidos.
c) ( ) seus processos são monitorados e medidos e deseja-se atingir um nível em que estes sejam documentados e comunicados.
d) ( ) boas práticas são seguidas e automatizadas, e deseja-se atingir um nível em que seus processos sejam documentados e medidos.
e) ( ) não há gestão em seus processos e se deseja atingir um nível em que estes sejam monitorados e medidos.

15) Ainda no cenário anterior, qual o modelo que deveria ser indicado, e por qual motivo, se a maioria dos projetos fosse de sistemas e de *software*?

Gabarito

Confira, a seguir, as respostas corretas para as questões autoavaliativas propostas:

10) c.

14) a.

9. CONSIDERAÇÕES FINAIS

Nesta unidade, foram abordados e apresentados os conceitos teóricos e os modelos de aplicabilidade relacionados à implantação da Governança de TI para as diversas áreas que nela existem, focando o detalhamento dos modelos de boas práticas COBIT e ITIL, bem como os benefícios que ambos podem trazer quando corretamente implementados dentro das organizações.

Uma vez apresentados tais fundamentos, aconselha-se a constante atualização acerca dos diversos modelos praticados pelo mercado profissional, bem como a motivação para que você busque as certificações necessárias para a comprovação dos conhecimentos.

10. E-REFERÊNCIAS

Lista de figuras

Figura 2 *Áreas-Foco da Governança de TI na visão do COBIT*. Disponível em: <http://www.isaca.org/Knowledge-Center/COBIT/Documents/COBIT-4.1-Brochure.pdf>. Acesso em: 19 set. 2011.

Figura 3 *Os quatro domínios inter-relacionados do COBIT*. Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-portuguese.pdf?id=82655ff9-2aa9-44ed-9fe8-d8c16599ed75>. Acesso em: 9 ago. 2011.

11. REFERÊNCIAS BIBLIOGRÁFICAS

CAMPOS, A. L. N. *Sistema de segurança da informação*: controlando os riscos. [s.l.]: Visual Books, 2007. p. 125-126.

CARUSO, C. A. A.; STEFFEN, F. D. *Segurança em informática e de informações*. 2. ed. rev. e ampl. São Paulo: Senac, 1999.

FERNANDES, A. A.; ABREU, V. F. *Implantando a governança de TI*: da estratégia à gestão dos processos e serviços. 2. ed. Rio de Janeiro: Brasport, 2008.