UNIDADE 1

1

Introdução à auditoria de sistemas informatizados

Objetivos de aprendizagem

Ao final desta unidade, você terá subsídios para:

- contextualizar a evolução dos sistemas computacionais e da necessidade da segurança da informação.
- entender o conceito de auditoria e, mais especificamente, da auditoria de sistemas informatizados.
- compreender a importância da auditoria de sistemas informatizados.
- conhecer os desafios éticos e sociais da tecnologia da informação.

Seções de estudo

Apresentamos, a seguir, as seções para você estudar.

Seção 1 Evolução dos sistemas computacionais e de segurança da informação

Seção 2 Quais são os conceitos básicos da auditoria?

Seção 3 Qual é o tipo da auditoria objeto deste estudo?

Seção 4 Por que auditar?

Seção 5 Quais são os desafios éticos da auditoria de sistemas informatizados?

Após a leitura dos conteúdos, realize as atividades de auto-avaliação propostas no final da unidade e no EVA.

Para início de estudo

Para você que está prestes a iniciar os estudos na área de auditoria, algumas considerações são necessárias.

Esta unidade pretende conceituar a auditoria de sistemas informatizados. Para que o seu conceito e importância fiquem claros, na primeira seção será abordada a evolução dos sistemas de informação.

Nas terceira e quarta seções são enfocados os desafios éticos que permeiam a tecnologia de informação e a importância da auditoria nos sistemas informatizados.

Bom estudo!

Seção 1 – Evolução dos sistemas computacionais e dos de segurança da informação

Nem sempre o bem mais precioso de uma empresa se encontra no final da sua linha de produção, na forma de um produto acabado ou de algum serviço prestado Ele pode estar nas informações relacionadas a este produto ou serviço.

A crescente utilização de soluções informatizadas nas diversas áreas de serviços exige níveis de segurança adequados e maior exposição dos valores e informações. A evolução da tecnologia de informação, migrando de um ambiente centralizado para um ambiente distribuído, interligando redes internas e externas, somada à revolução da Internet, mudou a forma de se fazer negócios. Isto fez com que as empresas se preocupassem mais com o controle de acesso às suas informações bem como a proteção dos ataques, tanto internos quanto externos.

Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e o uso de computadores de grande porte, a estrutura de segurança já ficou um pouco

mais sofisticada, englobando controles lógicos, porém ainda centralizados. (CRONIN, 1996)

Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes cada vez mais especializadas para a sua implementação e gerência.

Paralelamente, os sistemas de informação também adquiriram uma importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável.

A esta constatação, você pode adicionar o fato de que hoje em dia não existem mais empresas que não dependam da tecnologia da informação, num maior ou menor grau. Pelo fato de que esta mesma tecnologia permitiu o armazenamento de grande quantidade de informações em um local restrito e centralizado, criou-se aí uma grande oportunidade ao acesso não autorizado.

A segurança da informação tornou-se estratégica, pois interfere na capacidade das organizações de realizarem negócios e no valor de seus produtos no mercado.

Em tempos de economia nervosa e racionalização de investimentos, a utilização de recursos deve estar focada naquilo que mais agrega ao valor do negócio.

Visando minimizar as ameaças, a ISO (International Standardization Organization) e a ABNT (Associação Brasileira de Normas Técnicas), em sintonia com a ISO, publicaram uma norma internacional para garantir a segurança das informações nas empresas, a ISO 17799:1. As normas ISO e ABNT são resultantes de um esforço internacional que consumiu anos de pesquisa e desenvolvimento para se obter um modelo de segurança eficiente e universal.

Quais são as ameaças?

Este modelo tem como característica principal tentar preservar a disponibilidade, a integridade e o caráter confidencial da informação.

- O **comprometimento do sistema de informações**, por problemas de segurança, pode causar grandes prejuízos à organização. Diversos tipos de incidentes podem ocorrer a qualquer momento, podendo atingir a informação confidencial, a integridade e disponibilidade.
- Problemas de **quebra de confidência,** por vazamento ou roubo de informações sigilosas, podem expor para o mercado ou concorrência as estratégias ou tecnologias da organização, eliminando um diferencial competitivo, comprometendo a sua eficácia, podendo perder mercado e até mesmo ir à falência.
- **Problemas de disponibilidade** podem ter um impacto direto sobre o faturamento, pois deixar uma organização sem matéria-prima ou sem suprimentos importantes ou mesmo, o impedimento de honrar compromissos com clientes, prejudicam sua imagem perante os clientes, gerando problemas com custos e levando a margem de lucro a ficar bem comprometida.
- **Problemas de integridade**, causados por invasão ou fatores técnicos em dados sensíveis, sem uma imediata percepção, irão impactar sobre as tomadas de decisões. Decisões erradas fatalmente reduzirão o faturamento ou aumentarão os custos, afetando novamente a margem de lucros.
- A **invasão da página de Internet de uma empresa**, com modificação de conteúdo, ou até mesmo a indisponibilidade de serviços on-line, revela a negligência com a segurança da informação e causa perdas financeiras a quem sofreu algum tipo de ataque.

Contudo, você pode inferir que elementos fundamentais para a sobrevivência das empresas estão relacionados com segurança da informação, a qual contribui muito para a sua lucratividade e sobrevivência, ou seja, agrega valor ao negócio e garante o retorno do investimento feito.

Agora que você pode entender a importância para uma organização de tomar medidas para salvaguardar suas informações, acompanhe, na próxima seção, conceitos básicos para quem começa a estudar auditoria.

Seção 2 – Quais são os conceitos básicos da auditoria?

Alguns conceitos básicos relacionados com a auditoria são: campo, âmbito e área de verificação.

- O **campo** compõe-se de aspectos como: objeto, período e natureza da auditoria.
- O **objeto** é definido como o "alvo" da auditoria, pode ser uma entidade completa (corporações públicas ou privadas, por exemplo).
- **Período** a ser fiscalizado pode ser um mês, um ano ou, em alguns casos, poderá corresponder ao período de gestão do administrador da instituição.
- A **natureza** da auditoria poderá ser operacional, financeira ou de legalidade, por exemplo. Na seqüência, você estudará com mais detalhes a natureza (ou tipo) da auditoria.
- O **âmbito da auditoria** pode ser definido como a amplitude e exaustão dos processos de auditoria, ou seja, define o limite de aprofundamento dos trabalhos e o seu grau de abrangência.
- A **área de verificação** pode ser conceituada como sendo o conjunto formado pelo campo e âmbito da auditoria.

A auditoria é uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com o objetivo de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas ou padrões.

Os procedimentos de auditoria formam um conjunto de verificações e averiguações que permite obter e analisar as informações necessárias à formulação da opinião do auditor.

- **Controle** é a fiscalização exercida sobre as atividades de pessoas, órgãos, departamentos ou sobre produtos, para que estes não se desviem das normas ou objetivos previamente estabelecidos. Existem três tipos de controles.

Preventivos	usados para prevenir fraudes, erros ou vulnerabilidades. (senhas de acesso a algum sistema informatizado, por exemplo)
Detectivos	usados para detectar fraudes, erros, vulnerabilidades (por exemplo: Log de eventos de tentativas de acesso a um determinado recurso informatizado)
Corretivos	usados para corrigir erros ou reduzir impactos causados por algum sinistro (planos de contingência, por exemplo)

Um dos objetivos desses controles é, primeiramente, a manutenção do investimento feito pela corporação em sistemas informatizados, tendo em vista que os sistemas de informação interconectados de hoje desempenham um papel vital no sucesso empresarial de um empreendimento.

A internet e as redes internas similares, ou intranets, e as redes interorganizacionais externas, as chamadas extranets, podem fornecer a infra-estrutura de informação que uma empresa necessita para operações eficientes, administração eficaz e vantagem competitiva. Entretanto, os sistemas de informação também precisam apoiar as estratégias de negócios, os processos empresariais e as estruturas organizacionais e culturais de um empreendimento.

Esses controles também têm como objetivo evitar que algum sinistro venha a ocorrer; não conseguindo evitar, tentar fazer com que o impacto seja pequeno e, se mesmo assim, o impacto for grande, ter em mãos processos que auxiliem a reconstrução do ambiente.

O que precisa ser controlado?

Em geral, é um *check-list* que contempla os itens a serem verificados durante a auditoria. A concepção desses procedimentos antes do início dos processos de auditoria é de suma importância porque garantirá um aumento da produtividade e da qualidade do trabalho. Como exemplo, pode-se citar que, para o bom andamento de uma partida de futebol, não é aconselhável mudar as regras do jogo enquanto o mesmo estiver acontecendo; faz-se isto antes de começar a partida.

Os chamados "achados" de auditoria são fatos importantes observados pelo auditor durante a execução dos trabalhos.

Apesar de que geralmente são associados a falhas ou vulnerabilidades, os "achados" podem indicar pontos fortes da corporação auditada. Para que eles façam parte do relatório final de auditoria, os mesmos devem ser relevantes e baseados em fatos e evidências incontestáveis.

Os papéis de trabalho são registros que evidenciam atos e fatos observados pelo auditor.

Esses registros podem estar em forma de documentos, tabelas, listas de verificações, planilhas, arquivos, entre outros. Estes documentos são a base para o relatório de auditoria, pois contêm registro da metodologia utilizada, procedimentos, fontes de informação, enfim, todas as informações relacionadas ao trabalho de auditoria.

Já na fase da concepção do relatório, são feitas as recomendações de auditoria.

Elas são medidas corretivas possíveis, sugeridas pela instituição fiscalizadora ou pelo auditor em seu relatório, para corrigir as deficiências detectadas durante o trabalho de verificação de vulnerabilidades ou deficiências. Dependendo da competência ou posição hierárquica do órgão fiscalizador, essas recomendações podem se transformar em determinações a serem cumpridas. (DIAS, 2000)

Seção 3 – Qual é o tipo de auditoria objeto deste estudo?

Vários autores fazem uma classificação ou denominação formal sobre a natureza ou sobre os diversos tipos de auditorias existentes. Os tipos mais comuns são classificados quanto: à forma de abordagem, ao órgão fiscalizador e à área envolvida. Acompanhe, a seguir, quais são elas:

Tabela 1 – Classificação dos tipos de auditoria

Classificação	Tipos de auditoria	Descrição
Quanto à forma de abordagem:	**Auditoria horizontal**	auditoria com tema específico, realizada em várias entidades ou serviços paralelamente.
	Auditoria orientada	focaliza uma atividade específica qualquer ou atividades com fortes indícios de fraudes ou erros.
Quanto ao órgão fiscalizador:	**Auditoria interna**	auditoria realizada por um departamento interno, responsável pela verificação e avaliação dos sistemas e procedimentos internos de uma entidade. Um de seus objetivos é reduzir a probabilidade de fraudes, erros, práticas ineficientes ou ineficazes. Este serviço deve ser independente e prestar contas diretamente à classe executiva da corporação.
	Auditoria externa	auditoria realizada por uma empresa externa e independente da entidade que está sendo fiscalizada, com o objetivo de emitir um parecer sobre a gestão de recursos da entidade, sua situação financeira, a legalidade e regularidade de suas operações.
	Auditoria articulada	trabalho conjunto de auditorias internas e externas, devido à superposição de responsabilidades dos órgãos fiscalizadores, caracterizado pelo uso comum de recursos e comunicação recíproca dos resultados.

Quanto à área envolvida	**Auditoria de programas de governo**	Acompanhamento, exame e avaliação da execução de programas e projetos governamentais. Auditoria do planejamento estratégico – verifica se os principais objetivos da entidade são atingidos e se as políticas e estratégias são respeitadas.
	Auditoria administrativa	engloba o plano da organização, seus procedimentos, diretrizes e documentos de suporte à tomada de decisão.
	Auditoria contábil	é relativa à fidedignidade das contas da instituição. Esta auditoria, consequentemente, tem como finalidade fornecer alguma garantia de que as operações e o acesso aos ativos se efetuem de acordo com as devidas autorizações.
	Auditoria financeira	conhecida também como auditoria das contas. Consiste na análise das contas, da situação financeira, da legalidade e regularidade das operações e aspectos contábeis, financeiros, orçamentários e patrimoniais, verificando se todas as operações foram corretamente autorizadas, liquidadas, ordenadas, pagas e registradas. Auditoria de legalidade – conhecida como auditoria de conformidade. Consiste na análise da legalidade e regularidade das atividades, funções, operações ou gestão de recursos, verificando se estão em conformidade com a legislação em vigor.
	Auditoria operacional	incide em todos os níveis de gestão, nas fases de programação, execução e supervisão, sob a ótica da economia, eficiência e eficácia. Analisa também a execução das decisões tomadas e aprecia até que ponto os resultados pretendidos foram atingidos.
	Auditoria de sistemas informatizados	tipo de auditoria essencialmente operacional, por meio da qual os auditores analisam os sistemas de informática, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e deficiências.

Destas auditorias, qual delas é o seu objeto de estudo?

É a auditoria de sistemas informatizados. E como já foi conceituada, a auditoria de sistemas informatizados é um tipo de auditoria operacional, ou seja, analisa a gestão de recursos, focalizando os aspectos de eficiência, eficácia, economia e efetividade.

Dependendo da área de verificação escolhida, este tipo de auditoria pode abranger:

- todo o ambiente de informática ou
- a organização do departamento de informática. Além disso, pode ainda contemplar:
- os controles sobre banco de dados, redes de comunicação e de computadores e
- controles sobre os aplicativos.

Deste modo, sob o ponto de vista dos tipos de controles citados, a auditoria pode ser separada em duas grandes áreas:

- Auditoria de segurança de informações - este tipo de auditoria em ambientes informatizados determina a postura ou situação da corporação em relação à segurança. Avalia a política de segurança e os controles relacionados com aspectos de segurança, enfim, controles que influenciam o bom funcionamento dos sistemas de toda a organização. São estes:
  - Avaliação da política de segurança.
  - Controles de acesso lógico.
  - Controles de acesso físico.
  - Controles ambientais.
  - Plano de contingência e continuidade de serviços.
  - Controles organizacionais.
  - Controles de mudanças.
  - De operação dos sistemas.
  - Controles sobre o banco de dados.
  - Controles sobre computadores.
  - Controles sobre ambiente cliente-servidor.

- Auditoria de aplicativos - este tipo de auditoria está voltado para a segurança e o controle de aplicativos específicos, incluindo aspectos que fazem parte da área que o aplicativo atende, como: orçamento, contabilidade, estoque, marketing, RH, etc. A auditoria de aplicativos compreende:
  - Controles sobre o desenvolvimento de sistemas aplicativos.
  - Controles de entrada, processamento e saída de dados.
  - Controles sobre o conteúdo e funcionamento do aplicativo com relação à área por ele atendida.

Esses tipos de auditoria são comumente usados para se alcançarem altos padrões de qualidade no desenvolvimento de softwares: o mais famoso desses modelos é o CMM. (DIAS, 2000)

Uma vez compreendida a abrangência e o escopo da auditoria dos sistemas informatizados, compreenda, na seção seguinte, por que auditar.

Seção 4 – Por que auditar?

Um ditado popular diz que nenhuma corrente é mais forte que seu elo mais fraco; da mesma forma, nenhuma parede é mais forte que a sua porta ou janela mais fraca, de modo que você precisa colocar as trancas mais resistentes possíveis nas portas e janelas. De forma similar é o que acontece quando você implementa segurança em um ambiente de informações. Na realidade, o que se procura fazer é eliminar o máximo possível de pontos fracos ou garantir o máximo de segurança possível para os mesmos.

Acima de tudo, o bem mais valioso de uma empresa pode não ser o produzido pela sua linha de produção ou o serviço prestado, mas as informações relacionadas com este bem de consumo ou serviço. Ao longo da história, o ser humano sempre buscou o controle das

informações que lhe eram importantes de alguma forma; isto é verdadeiro mesmo na mais remota antiguidade. O que mudou desde então foram as formas de registros e armazenamento das informações; se na pré- história e até mesmo nos primeiros milênios da idade antiga o principal meio de armazenamento e registro de informações era a memória humana, com o advento dos primeiros alfabetos isto começou a mudar. Mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas.

Atualmente, não há organização humana que não seja altamente dependente da tecnologia de informações, em maior ou menor grau. E o grau de dependência agravou-se muito em função da tecnologia de informática, que permitiu acumular grandes quantidades de informações em espaços restritos. O meio de registro é, ao mesmo tempo, meio de armazenamento, meio de acesso e meio de divulgação.

Esta característica traz conseqüências graves para as organizações, por facilitar os ataques de pessoas não-autorizadas.

Por exemplo, um banco não trabalha exatamente com dinheiro, mas com informações financeiras relacionadas com valores seus e de seus clientes. A maior parte destes dados é de natureza sigilosa, por força de determinação legal ou por se tratarem de informações de natureza pessoal, que controlam ou mostram a vida econômica dos clientes, os quais podem vir a sofrer danos, caso elas sejam levadas a público.

Independente do setor da economia em que a empresa atue, as informações estão relacionadas com seu processo de produção e de negócios, políticas estratégicas, de marketing, cadastro de clientes, etc. Não importa o meio físico em que as informações estão armazenadas, elas são de valor inestimável não só para a empresa que as gerou, como também para seus concorrentes. Em último caso, mesmo que as informações não sejam sigilosas, na maioria das vezes elas estão relacionadas com atividades diárias da empresa que, sem elas, poderia ter dificuldades.

Tradicionalmente, as empresas dedicam grande atenção de seus ativos físicos e financeiros, mas pouca ou até mesmo nenhuma atenção aos ativos de informação que possuem; esta proteção tradicional pode nem mesmo visar um bem valioso. Da mesma forma que seus ativos tangíveis, as informações envolvem três fatores de produção tradicionais: capital, mão-de-obra e processos. Assim, ainda que as informações não sejam passíveis do mesmo tratamento fisco-contábil que os outros ativos, do ponto de vista do negócio, elas são um ativo da empresa e, portanto, devem ser protegidas. Isto vale tanto para as informações como para seus meios de suporte, ou seja, para todo o ambiente de informações. (O`BRIEN, 2002).

A figura 1.1 mostra os fatores econômicos de uma organização, onde o capital, a mão-de-obra e os processos geram os ativos de uma empresa, ou seja, os produtos, os bens e a informações.

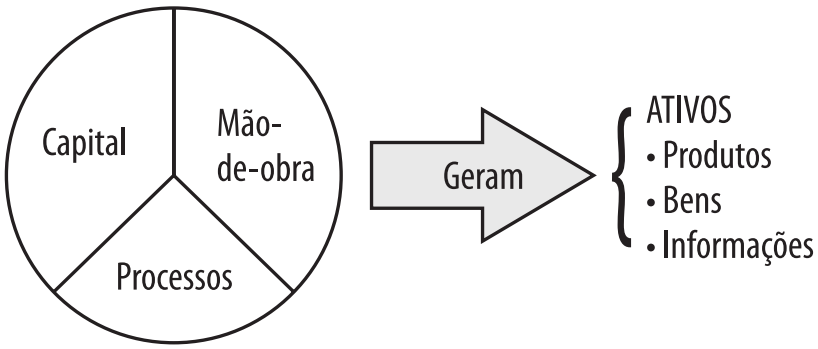

Figura 1.1 – Fatores econômicos de produção.
Fonte: Caruso&Steffen (1999)

Numa instituição financeira, o ambiente de informações não está apenas restrito à área de informática, ele chega a mais longínqua localização geográfica onde haja uma agência ou representação de qualquer tipo. Enquanto na área de informática os ativos de informação estão armazenados, em sua maior parte, em meios magnéticos, nas áreas fora deste ambiente eles ainda estão representados em grande parte por papéis, sendo muito tangíveis e de entendimento mais fácil por parte de seres humanos.

É importante ressaltar que muitas empresas não sobrevivem mais que poucos dias a um colapso do fluxo de informações, não importando o meio de armazenamento das informações.

E, dada à característica de tais empreendimentos, que no caso de bancos é essencialmente uma relação de confiança, é fácil prever que isto acarretaria completo descontrole sobre os negócios e até uma corrida ao caixa. A atual dependência das instituições financeiras em relação à informática está se estendendo por toda a economia, tornando aos poucos todas as empresas altamente dependentes dos computadores e, conseqüentemente, cada vez mais sensíveis aos riscos representados pelo eventual colapso do fluxo de informações de controle gerencial.

Os riscos são agravados em progressão geométrica à medida que informações essenciais ao gerenciamento dos negócios são centralizadas e, principalmente, com o aumento do grau de centralização. Ainda que estes riscos sejam sérios, as vantagens dessa centralização são maiores, tanto sob aspectos econômicos, quanto sob aspectos de agilização de processos de tomada de decisão em todos os níveis. Esta agilização é tanto mais necessária, quanto maior for o uso de facilidades de processamento de informação pelos concorrentes.

É preciso, antes de qualquer coisa, cercar o ambiente de informações com medidas que garantam sua segurança efetiva a um custo aceitável, pois é impossível obter-se segurança total já que, a partir de um determinado nível, os custos envolvidos tornam-se cada vez mais onerosos e superam os benefícios obtidos. Estas medidas devem estar claramente descritas na política global de segurança da organização, delineando as responsabilidades de cada grau da hierarquia e o grau de delegação de autoridade e, muito importante, estarem claramente sustentadas pela alta direção.

A segurança, mais que estrutura hierárquica, os homens e os equipamentos envolvem uma postura gerencial, que ultrapassa a tradicional abordagem da maioria das empresas.

Dado ao caráter altamente dinâmico que as atividades relacionadas com o processamento de informações adquiriram ao longo do tempo, a política de segurança de informações deve ser a mais ampla e mais simples possível.

Como conseqüência da informatização, outros aspectos começam a ser levantados, o acúmulo centralizado de informação, causando um sério problema para a segurança.

Os riscos inerentes ao processo agravaram-se e um estudo mais detalhado sobre eles teve que ser realizado.

Uma pesquisa realizada pela Módulo Security Solutions aponta os potenciais riscos aos quais a informação está sujeita. A figura 2 mostra que a principal ameaça às organizações é o vírus de computador.

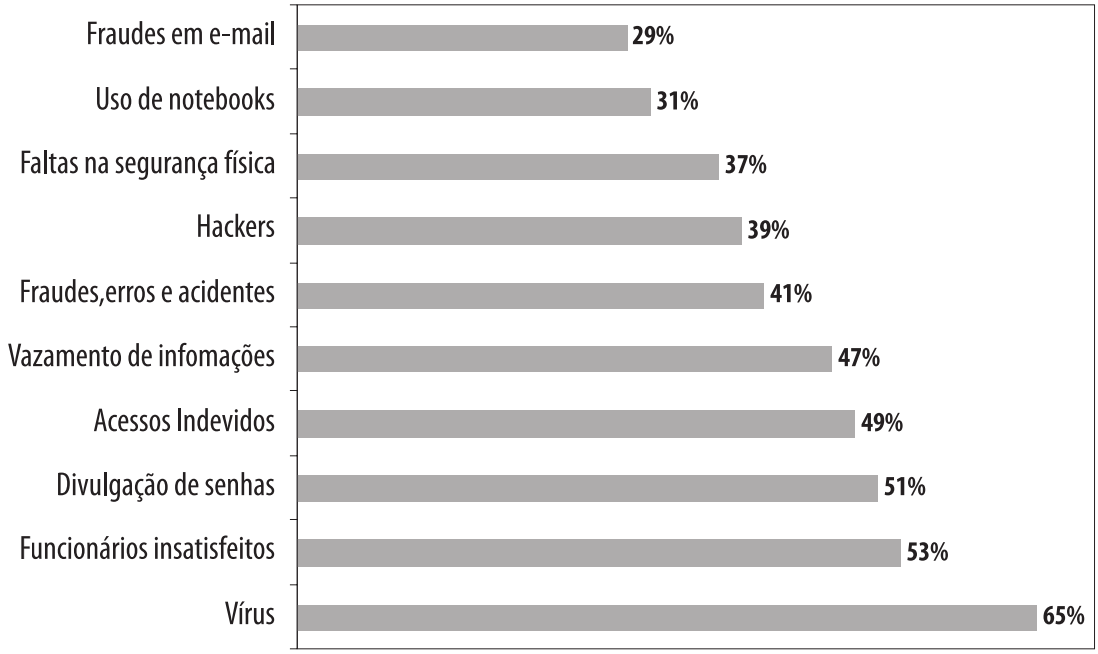

Figura 1.2 – Principais ameaças às informações nas organizações
Fonte: 9ª Pesquisa Nacional sobre Segurança da Informação – Módulo Security Solutions (2003)

As ameaças podem ser definidas como sendo agentes ou condições incidentes que comprometem as informações e seus ativos, por meio da exploração de vulnerabilidades.

O que caracteriza as vulnerabilidades?

As vulnerabilidades podem ser conceituadas como sendo fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações, que podem ser exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: caráter confidencial, integridade e disponibilidade.

As vulnerabilidades por si só não provocam incidentes de segurança, porque são elementos passivos. Porém, quando possuem um agente causador, como ameaças, esta condição favorável causa danos ao ambiente.

As vulnerabilidades podem ser:

Físicas	■ instalações prediais fora do padrão; ■ salas de CPD mal planejadas; ■ a falta de extintores, detectores de fumaça e outros para combate a incêndio em sala com armários e fichários estratégicos; ■ risco de explosões, vazamentos ou incêndio.
Naturais	■ os computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades, e ■ outros, como falta de energia, o acúmulo de poeira, o aumento de umidade e de temperatura, etc.
Hardware	■ falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação.
Software	■ erros na aquisição de softwares sem proteção ou na configuração podem ter como conseqüência uma maior quantidade de acessos indevidos, vazamentos de informações, perda de dados ou indisponibilidade do recurso quando necessário.
Mídias	■ discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.
Comunicação	■ acessos de intrusos ou perda de comunicação.
Humanas	■ rotatividade de pessoal, ■ falta de treinamento, ■ compartilhamento de informações confidenciais na execução de rotinas de segurança, ■ erros ou omissões; ■ ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismos, roubos, destruição da propriedade ou dados, invasões ou guerras.

O que é ser *Hacker*?

O termo genérico para identificar quem realiza ataques em um sistema de computadores é *hacker*. Porém, esta generalização possui diversas ramificações, pois cada ataque apresenta um objetivo diferente.

Por definição, *hacker* são aqueles que utilizam seus conhecimentos para invadir sistemas, sem a intenção de causar danos às vítimas, mas como um desafio às suas habilidades.

Os *hacker*s possuem grande conhecimento de sistemas operacionais e linguagens de programação. Constantemente buscam mais conhecimento, compartilham o que descobrem e jamais corrompem dados intencionalmente.

O termo *hacker* também é definido pela RFC-2828 (2000) como sendo alguma pessoa com um grande interesse e conhecimento em tecnologia, não utilizando eventuais falhas de seguranças descobertas em benefício próprio.

Como se tornou um termo genérico para invasores de redes, o termo *hacker* freqüentemente é usado para designar os elementos que invadem sistemas para roubar informações e causar danos.

O termo correto para este tipo de invasor seria *cracker* ou *intruder*, que também é utilizado para designar àqueles que decifram códigos e destroem proteções de softwares.

O termo *cracker* ou *intruder* é definido pela RFC-2828 como sendo alguém que tenta quebrar a segurança ou ganhar acesso a sistemas de outras pessoas sem ser convidado, não sendo, obrigatoriamente, uma pessoa com grande conhecimento de tecnologia como o *hacker*.

O termo *hacker* existe desde o ano de 1960. A palavra começou a ser usada pelos membros do *Tech Model Rail Club*, do Instituto de Tecnologia de Massachusetts (MIT), e indicava pessoas com capacidades técnicas para proezas que ninguém mais conseguia. Na área de informática, este termo foi usado para designar programadores prodigiosos, de técnica apurada, visivelmente superior.

Podemos classificar essas pessoas em várias categorias:

- *Carders* – Aqueles que fazem compras com cartão de crédito alheio ou gerado, ou seja, os *carders* têm grande facilidade em fazer compras via internet ou em outro meio.
- *Hacker*s – Pessoas com um grande interesse e conhecimento em tecnologia, não utilizando eventuais falhas de seguranças em benefício próprio. Porém, não destroem dados.
- *Crackers* – Os crackers são como os *hacker*s, porém gostam de ver a destruição. Eles invadem e destroem só para ver o caos formado. Eles apagam todo o sistema sempre deixando a sua marca registrada.
- *Phreacking* – São os piratas da telefonia. Eles fazem tudo o que é relativo aos telefones, convencionais ou celulares. (SPYMAN, 2002).

Existem muitas maneiras de se atacar os sistemas de informação de uma organização. Na figura 3 está disponibilizada uma pesquisa mostrando um balanço dos tipos de ataques mais usados nos cinco últimos anos. Esta pesquisa foi realizada pelo departamento de crimes de computador do FBI.

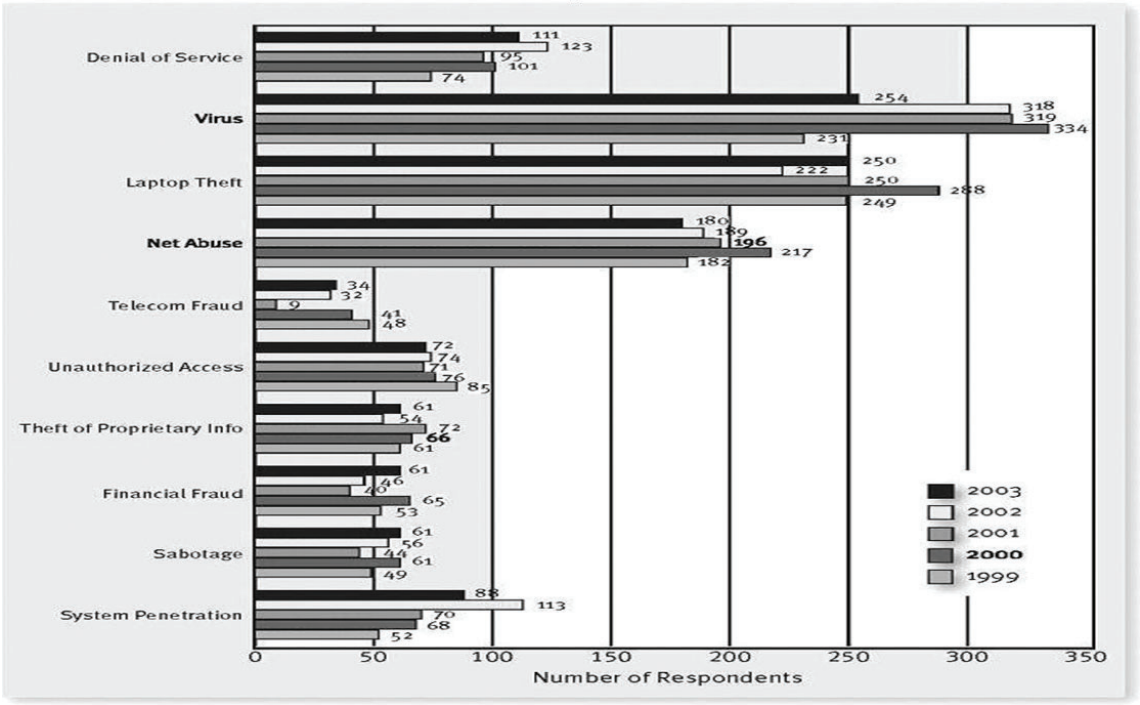

Figura 3 – Tipos de ataques mais utilizados
Fonte: CSI/FBI 2003 Computer Crime and Security Survey (2003)

As mais famosas técnicas de ataques às redes corporativas são:

- **Quebra de Senha** – O quebrador de senha, ou cracker, é um programa usado pelo *hacker* para descobrir uma senha do sistema. Uma das formas de quebra são os testes de exaustão de palavras, a decodificação criptográfica, etc.

- ***Denial of Service*** – Também conhecido como DoS, estes ataques de negação de serviço são aborrecimentos semelhantes aos *mails* bomba, porém muito mais ameaçadores porque eles podem incapacitar temporariamente uma rede corporativa ou um provedor de acesso. É um ataque que consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Sua finalidade não é o roubo de dados, mas a indisponibilidade de serviço. Existem variantes deste ataque, como o DoS distribuído, chamado DDoS, ou seja, a tentativa de sobrecarregar o I/O de algum serviço é feita de vários locais ao mesmo tempo.

- **Cavalo de tróia** – É um programa disfarçado que executa alguma tarefa maligna. Um exemplo, o usuário roda um jogo qualquer que foi pego na internet. O jogo instala o cavalo-de-tróia, que abre uma porta TCP (*Transmission Control Protocol*) no micro para a invasão. Este software não propaga a si mesmo de um computador para outro. Há também o cavalo-de-tróia dedicado a roubar senhas e outros dados.

- ***Mail Bomb*** – É considerado como dispositivo destrutivo. Utiliza a técnica de inundar um computador com mensagens eletrônicas. Em geral, o agressor usa um script para gerar um fluxo contínuo de mensagens e abarrotar a caixa postal de alguém. A sobrecarga tende a provocar uma negação de serviço, ou um DoS no servidor de correio eletrônico. Não há perda de dados na maioria dos casos.

- ***Phreacking*** – é o uso indevido das linhas telefônicas, fixas e celulares. No passado, os *phreackers* empregavam gravadores de fita e outros dispositivos para produzir sinais de controle e enganar o sistema de telefonia. Conforme as companhias telefônicas foram reforçando a segurança, as técnicas foram ficando cada vez mais difíceis. Hoje em dia é uma atividade muito elaborada, que poucos conhecem.

- **Scanners de Porta** – São programas que buscam portas TCP abertas por onde pode ser feita uma invasão. Para que a varredura não seja percebida pela vítima, alguns scanners testam as portas de um computador durante muitos dias, em horários aleatórios.

- ***Smurf*** – É outro tipo de ataque de negação de serviço. O agressor envia uma rápida seqüência de solicitações de *ping* (um teste para verificar se um servidor está acessível) para um endereço de *brodcast*. Usando *spoofing*, o *cracker* faz com que o servidor de *broadcast* encaminhe as respostas não para o seu endereço, mas para o da vítima. Assim o computador alvo é inundado pelo *Ping*.

- ***Spoofing*** – É a técnica de se fazer passar por outro computador da rede para conseguir acesso a um sistema. Há muitas variantes, como o *spoofing* de IP. Para executá-lo, o invasor altera o cabeçalho dos pacotes IP, de modo que pareça estar vindo de uma outra máquina, possivelmente, uma que tenha cesso liberado.
- ***Sniffer*** – É um programa ou dispositivo que analisa o tráfego na rede. *Sniffer*s são úteis e usados normalmente para o gerenciamento de redes. Porém nas mãos erradas, é uma ferramenta poderosa no roubo de informações sigilosas.
- **Vírus** – São programas desenvolvidos para alterar softwares instalados em um computador, ou mesmo apagar todas as informações existentes no computador. Possuem comportamento semelhante ao vírus biológico, multiplicam-se, precisam de hospedeiros, esperam o momento certo para o ataque e tentam se esconder para não serem exterminados. A internet e o correio eletrônico são hoje os principais meios de propagação de vírus. A RFC-2828 define vírus como sendo um software com a capacidade de se duplicar, infectando outros programas. Um vírus não pode se auto-executar, requer que o programa hospedeiro seja executado para ativá-lo.
- ***Worm*** – São programas auto-replicantes que não alteram arquivos, mas residem na memória ativa e se duplicam por meio de redes de computador. Os *worm*s utilizam recursos do sistema operacional para ganhar acesso ao computador e, ao se replicarem, usam recursos do sistema, tornando as máquinas lentas e interrompendo outras funções. Um *worm* é um programa de computador que pode se auto-executar, propagar-se pelos computadores de uma rede, podendo consumir os recursos do computador destrutivamente (RFC-2828, 2000).

Após ter acompanhado esta série de possíveis vulnerabilidades, acreditamos que você esteja convencido de que auditar é preciso, não é mesmo?

Auditar é preciso porque o uso inadequado dos sistemas informatizados pode impactar uma sociedade. Informação com pouca precisão pode causar a alocação precipitada de recursos dentro das corporações e as fraudes podem ocorrer devido à falta de sistemas de controle.

Então, para garantir que os investimentos feitos em tecnologia da informação retornem para a empresa na forma de lucros, custos menores e um menor custo total de propriedade é que o auditor de sistemas informatizados irá atuar. De posse dos objetivos, normas ou padrões da corporação o auditor irá verificar se tudo está funcionando como deveria.

Ainda para ilustrar a importância da atuação do auditor, acompanhe, na seqüência, algumas estatísticas sobre os ataques aos sistemas de informação.

A Tabela 2 mostra quais são as medidas tomadas pelas organizações no que diz respeito à segurança no ano de 2003.

Tabela 2 – As medidas de segurança mais utilizadas pelas empresas brasileiras no ano de 2003.

"TOP 10" MEDIDAS DE SEGURANÇA MAIS IMPLEMENTADAS		
Ranking 2003	Medidas de Segurança	%
1º	Antivírus	90
2º	Sistema de backup	76,5
3º	Firewall	75,5
4º	Política de segurança	72,5
5º	Capacitação técnica	70
6º	Software de controle de acesso	64
7º	Segurança física na sala de servidores	63
8º	Proxy server	62
9º	Criptografia	57
10º	Análise de riscos	56

Fonte: 9ª Pesquisa Nacional sobre Segurança da Informação – Módulo Security Solutions (2003)

O maior investimento em TI por profissionais da área foi em antivirus, já que uma grande quantidade de empresas tem sofrido ataques ou até mesmo deixou de ficar com seus serviços disponíveis. Logo em seguida, a maior preocupação são os sistemas de backup. E veja que a política de segurança está em quarto lugar.

Nota-se pela pesquisa da figura 5 que o roubo de informações e a negação de serviço, ou seja, parar de disponibilizar dados, informações e aplicações são os ataques que mais dão prejuízos para as organizações.

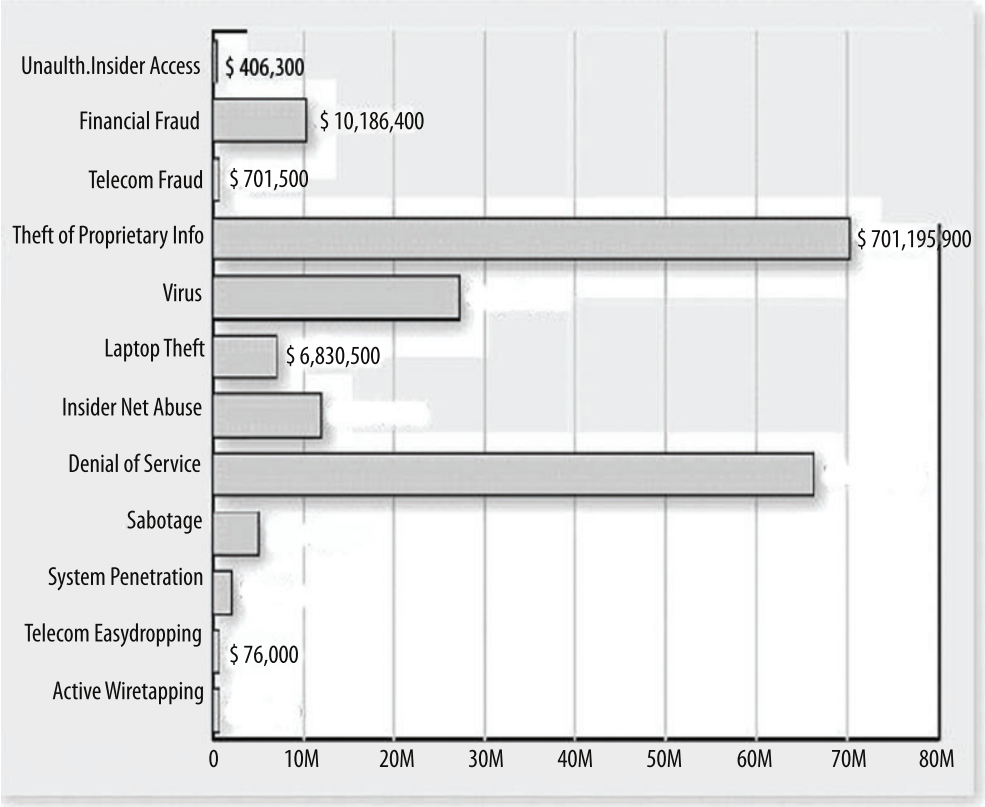

Figura 5 – Perdas financeiras relacionadas com os tipos de ataques realizados
Fonte: CSI/FBI 2003 Computer Crime and Security Survey (2003)

Apesar das vulnerabilidades, não são todas as empresas que prontamente investem em sistemas de segurança de informações, porque os responsáveis por manter o ambiente funcionando enfrentam algumas dificuldades para conseguir estes recursos.

Figura 6 – Principais obstáculos para a implementação da Segurança
Fonte: 9ª Pesquisa Nacional sobre Segurança da Informação – Módulo Security Solutions (2003)

Falta de consciência dos executivos (23%), dificuldade em demonstrar o retorno (18%) e custo de implementação (16%) foram considerados os três principais obstáculos para implementação da segurança nas empresas, como ilustrado na figura 7. (MÓDULO, 2003)

Quando questionados sobre a fonte de informações para se obter discernimento a respeito do que fazer quando se trata de segurança, os entrevistados se mostraram bastante informados a respeito, e apontaram as referências, normas e legislações que falam sobre o assunto.