Segurança em Tecnologia da Informação

Prof. Christian Meinecke Gross
Prof. Jan Charles Gross

UNIASSELVI
2013

Elaboração:

Prof. Christian Meinecke Gross

Prof. Jan Charles Gross

Revisão, Diagramação e Produção:

Centro Universitário Leonardo da Vinci – UNIASSELVI

Ficha catalográfica elaborada na fonte pela Biblioteca Dante Alighieri

UNIASSELVI – Indaial.

658.4038

G878s Gross, Christian Meinecke

Segurança em tecnologia da informação / Christian Meinecke Gross; Jan Charles Gross. Indaial : Uniasselvi, 2013.

244 p. : il

ISBN 978-85-7830-765-3

I. Tecnologia da informação.

II. Segurança.

1.Centro Universitário Leonardo da Vinci.

2. Gross, Christian Meinecke.

Apresentação

Caro(a) acadêmico(a)!

Estamos iniciando o estudo da disciplina Segurança em Tecnologia da Informação. Esta disciplina objetiva proporcionar uma aprendizagem autônoma sobre os principais conceitos de segurança na área da tecnologia da informação, proporcionando ao acadêmico o desenvolvimento de competências necessárias para a implementação da gestão da segurança da informação.

Neste contexto, o Caderno de Estudos de Segurança em Tecnologia da Informação está dividido em três unidades de estudo.

Iniciamos com a Unidade 1 apresentando os conceitos e as definições básicas da segurança da informação, tanto no aspecto lógico, físico e ambiental, bem como os métodos de segurança implementados nos processos realizados em sistemas de distribuídos.

Na Unidade 2 vamos conhecer os planos de continuidade operacional e de contingência, que consistem num conjunto de estratégias e procedimentos que deverão ser adotados quando do surgimento de problemas que comprometem o andamento normal dos processos. Ao final, serão apresentados os pontos relevantes para a definição da política de segurança da informação, que tem por objetivo estabelecer regras a fim de evitar e reduzir os riscos e ameaças em relação aos ativos da informação.

Na última unidade vamos estudar a auditoria de sistemas, que visa verificar se o ambiente informatizado garante a integridade dos dados manipulados pelo computador, através de procedimentos documentados e metodologias predefinidas, verificando aspectos de segurança e qualidade. Para isto, serão apresentadas as diversas normas e padrões de segurança que poderão ser adotados a fim de garantir que as metas da auditoria sejam alcançadas.

Buscando viabilizar a melhor apropriação dos conhecimentos, esta produção norteará os seus estudos.

Prof. Christian Meinecke Gross
Prof. Jan Charles Gross

Você já me conhece das outras disciplinas? Não? É calouro? Enfim, tanto para você que está chegando agora à UNIASSELVI quanto para você que já é veterano, há novidades em nosso material.

Na Educação a Distância, o livro impresso, entregue a todos os acadêmicos desde 2005, é o material base da disciplina. A partir de 2017, nossos livros estão de visual novo, com um formato mais prático, que cabe na bolsa e facilita a leitura.

O conteúdo continua na íntegra, mas a estrutura interna foi aperfeiçoada com nova diagramação no texto, aproveitando ao máximo o espaço da página, o que também contribui para diminuir a extração de árvores para produção de folhas de papel, por exemplo.

Assim, a UNIASSELVI, preocupando-se com o impacto de nossas ações sobre o ambiente, apresenta também este livro no formato digital. Assim, você, acadêmico, tem a possibilidade de estudá-lo com versatilidade nas telas do celular, *tablet* ou computador.

Eu mesmo, UNI, ganhei um novo *layout*, você me verá frequentemente e surgirei para apresentar dicas de vídeos e outras fontes de conhecimento que complementam o assunto em questão.

Todos esses ajustes foram pensados a partir de relatos que recebemos nas pesquisas institucionais sobre os materiais impressos, para que você, nossa maior prioridade, possa continuar seus estudos com um material de qualidade.

Aproveito o momento para convidá-lo para um bate-papo sobre o Exame Nacional de Desempenho de Estudantes – ENADE.

Bons estudos!

Olá acadêmico! Para melhorar a qualidade dos materiais ofertados a você e dinamizar ainda mais os seus estudos, a Uniasselvi disponibiliza materiais que possuem o código *QR Code*, que é um código que permite que você acesse um conteúdo interativo relacionado ao tema que você está estudando. Para utilizar essa ferramenta, acesse as lojas de aplicativos e baixe um leitor de *QR Code*. Depois, é só aproveitar mais essa facilidade para aprimorar seus estudos!

BATE PAPO SOBRE O ENADE!

Olá, acadêmico!

Você já ouviu falar sobre o **ENADE**?

Se ainda não ouviu falar nada sobre o ENADE, agora você receberá algumas informações sobre o tema.

Ouviu falar? Ótimo, este informativo reforçará o que você já sabe e poderá lhe trazer novidades.

Vamos lá!

Qual é o significado da expressão ENADE?

EXAME NACIONAL DE DESEMPENHO DOS ESTUDANTES

Em algum momento de sua vida acadêmica você precisará fazer a prova ENADE.

Que prova é essa?

É **obrigatória**, organizada pelo INEP – Instituto Nacional de Estudos e Pesquisas Educacionais Anisio Teixeira.

Quem determina que esta prova é obrigatória... O **MEC – Ministério da Educação**.

O objetivo do MEC com esta prova é o de avaliar seu desempenho acadêmico assim como a qualidade do seu curso.

Fique atento! Quem não participa da prova fica impedido de se formar e não pode retirar o diploma de conclusão do curso até regularizar sua situação junto ao MEC.

Não se preocupe porque a partir de hoje nós estaremos auxiliando você nesta caminhada.

Você receberá outros informativos como este, complementando as orientações e esclarecendo suas dúvidas.

Você tem uma trilha de aprendizagem do ENADE, receberá e-mails, SMS, seu tutor e os profissionais do polo também estarão orientados.

Participará de webconferências entre outras tantas atividades para que esteja preparado para #mandar bem na prova ENADE.

Nós aqui no NEAD e também a equipe no polo estamos com você para vencermos este desafio.

Conte sempre com a gente, para juntos mandarmos bem no ENADE!

UNIASSELVI

Sumário

UNIDADE 1

SEGURANÇA EM INFORMÁTICA

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, será possível:

- conhecer as principais características de segurança em um ambiente computacional e os principais motivadores de segurança;
- entender a importância dos controles e medidas de segurança física, lógica e ambiental, tendo em vista as diversas vulnerabilidades existentes;
- reconhecer os problemas relacionados à segurança dos sistemas distribuídos e as principais medidas de proteção.

PLANO DE ESTUDOS

Esta unidade está dividida em três tópicos, sendo que ao final de cada um deles, você encontrará atividades que auxiliarão na apropriação dos conhecimentos.

TÓPICO 1 – SEGURANÇA NO AMBIENTE COMPUTACIONAL

TÓPICO 2 – SEGURANÇA LÓGICA, FÍSICA E AMBIENTAL

TÓPICO 3 – SEGURANÇA EM SISTEMAS DISTRIBUÍDOS

Assista ao vídeo desta unidade.

TÓPICO 1

SEGURANÇA NO AMBIENTE COMPUTACIONAL

1 INTRODUÇÃO

Antes de iniciarmos nossos estudos em torno do assunto, é necessário entendermos o que significa segurança no ambiente computacional e conhecer algumas das consequências da utilização dos mesmos.

Este tópico, portanto, tem por finalidade apresentar a você os principais conceitos relacionados à segurança de um ambiente computacional, os principais motivadores e também os principais benefícios obtidos com a correta utilização de medidas de proteção no ambiente computacional.

O surgimento das redes de computadores e a interconexão destas aos meios de comunicação expuseram as informações mantidas por estas redes a inúmeros tipos de ataques e vulnerabilidades, dado o valor destas informações e sua importância para as empresas que as geraram e utilizam. O anonimato proporcionado por tais meios de comunicação, como por exemplo, a internet, torna ainda mais atrativo para pessoas mal intencionadas à busca por estas informações.

As empresas e instituições das mais diversas naturezas começaram a perceber os problemas relacionados à segurança no ambiente computacional, e buscam a cada dia mitigar e/ou eliminar os riscos relacionados às vulnerabilidades existentes, protegendo seus dados contra ataques.

2 SEGURANÇA E INFORMAÇÕES

Ao longo da história, o ser humano sempre buscou o controle sobre as informações que lhe eram importantes de alguma forma; isso é verdadeiro mesmo na mais remota Antiguidade.

> O que mudou desde então foram as formas de registro 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 isso começou a mudar. Mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas. (CARUSO; STEFFEN, 1999, p. 21).

Com uma tecnologia incipiente e materiais pouco apropriados para o registro de informações, de acordo com Caruso e Steffen (1999, p. 21), "era natural que o controle e a disseminação da tecnologia relacionada com as informações tornassem

o acesso a elas restritas a uma minoria sempre ligada ao grupo que dominava o poder econômico e político da sociedade".

Segundo Caruso e Steffen (1999, p. 21-22), "os primeiros suportes para registro de informações foram as paredes das habitações humanas". Somente com as mudanças tecnológicas nos meios de registro – as placas de barro dos sumérios, o papiro dos egípcios e o pergaminho – as informações passaram para meios de registro "portáveis". Mas foi com a disseminação da tecnologia de impressão e com a alfabetização mais ampla que as informações deixaram de ser "códigos" incompreensíveis. Somente nos últimos dois séculos a alfabetização começou a se espalhar por grandes segmentos da população de diversos países, e apenas em meados do século XX, a alfabetização se universalizou, ainda que grande parte da humanidade continue analfabeta.

Atualmente, conforme Caruso e Steffen (1999, p. 22), "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".

É evidente, segundo Gil (2000), que dependendo do porte e da área de atuação da organização, a forma e a intensidade do uso da computação diferem. Assim, temos as instituições financeiras que não conseguem funcionar nem poucas horas com a ausência dos computadores, bem como as microempresas que, apesar de poderem conviver com a ausência da tecnologia de PED, necessitam da participação de microcomputadores pessoais ou profissionais em suas atividades para possibilitar maior agilidade e diferenciação em relação a seus concorrentes.

PED - Processamento Eletrônico de Dados são atividades que utilizam a computação em seu processo.

Fontes (2006, p. 1) destaca três frases importantes sobre informação:

1. A informação, independente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos.

2. A informação tem valor para a organização.

3. Sem informação, a organização não realiza seu negócio.

Seja para um supermercadista preocupado com a gestão de seu estoque, seja para uma instituição bancária em busca da automação de suas agências bancárias, ou para uma indústria alimentícia prospectando a otimização da sua linha de produção. De acordo com Sêmola (2003, p. 2), "todos decidem suas ações e seus planos com base em informações".

Segundo Fontes (2006, p. 2), "informação é muito mais que um conjunto de dados. Transformar estes dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal ou profissional".

"Segurança da informação pode ser entendida como o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade". (BEAL, 2008, p. 1).

Segurança da informação objetiva, conforme Beal (2008, p. 1), a preservação de ativos de informações considerando três objetivos principais:

- Confidencialidade: garantir acesso à informação apenas aos seus usuários legítimos.
- Integridade: a informação deve ser verdadeira, estando correta (não corrompida), ou seja, é necessário garantir a criação legítima e consistente da informação ao longo do seu ciclo de vida: em especial, prevenindo contra criação, alteração ou destruição não autorizada de dados e informações. O objetivo de autenticidade da informação é englobado pelo da integridade, quando se pressupõe que este visa garantir que as informações permaneçam completas e precisas, e ainda que a informação obtida do ambiente externo também seja fidedigna como a criada internamente, produzida apenas por pessoas autorizadas e atribuída apenas ao seu legítimo autor.
- Disponibilidade: garantir que a informação e seus ativos associados estejam disponíveis aos usuários legítimos de modo oportuno para o funcionamento da organização e alcance de seus objetivos.

Para que a proteção da informação seja eficaz no dia a dia da organização, os conceitos e os regulamentos de segurança devem ser compreendidos e seguidos por todos os usuários. (FONTES, 2006, p. 10).

Complementarmente, Beal (2008, p. 1) informa que alguns autores acrescentam a esses três objetivos a legalidade (garantir que as informações foram produzidas em conformidade com a legislação), e o uso legítimo (garantir que os

recursos de informação não são utilizados por pessoas não autorizadas ou de modo não autorizado). No entendimento da autora, essas preocupações deveriam ser classificadas como objetivos organizacionais, visto que derivam dos requisitos de segurança necessários para proteger informações sob os pontos de vista já citados de confidencialidade, integridade e disponibilidade.

Fontes (2006, p. 12) cita que proteger a informação significa garantir, além das propriedades de confidencialidade, integridade e disponibilidade:

- Legalidade: o uso das informações deve estar de acordo com as leis aplicáveis, normas regulamentadoras, licenças, concessões, regimentos e contratos firmados, assim como com os princípios éticos seguidos pela organização e desejados pela sociedade.
- Auditabilidade: o acesso e uso das informações devem ser registrados, permitindo identificar quem a acessou e o que este fez com a informação obtida.
- Não repúdio de auditoria: o usuário gerador ou mantenedor da informação (uma mensagem de correio eletrônico ou algum arquivo texto) não pode negar o fato, visto a existência de mecanismos que garantam incontestavelmente a sua autoria.

O objetivo da legalidade, segundo Beal (2008, p. 2), "decorre da necessidade de a organização zelar para que as informações por ela ofertadas – em especial aquelas entregues a terceiros por determinação legal – sejam fidedignas e produzidas de acordo com as normas vigentes". Esse objetivo gera, no campo da segurança da informação, exigências no tocante à confidencialidade, integridade e disponibilidade de dados e informações (tais como requisitos de proteção do sigilo de informações pessoais, da consistência dos demonstrativos financeiros divulgados, da disponibilidade de serviços de informação e comunicação contratados por clientes). Da mesma forma, para garantir o objetivo organizacional de uso legítimo da informação, requisitos de confidencialidade, integridade e disponibilidade podem ser atribuídos a diferentes tipos de informação, de acordo com o papel que desempenham nos processos organizacionais.

Quando começamos a trabalhar em organizações, precisamos nos lembrar de que a informação é um bem, tem valor para a empresa e deve ser protegida. A informação deve ser cuidada por meio de políticas e regras, da mesma maneira que os recursos financeiro e material são tratados dentro da empresa. Com isso queremos dizer que a informação é um ativo de valor. É um recurso crítico para a realização do negócio e a execução da missão da organização. Portanto, sua utilização deve ter regras e procedimentos. (FONTES, 2006, p. 2).

Segundo Beal (2008), dados, informação e conhecimento, por sua alta capacidade de adicionar valor a processos, produtos e serviços, constituem recursos cada vez mais críticos para o alcance da missão e dos objetivos organizacionais. Como qualquer outro ativo valioso para as organizações, as informações críticas

para o negócio devem ser protegidas contra as ameaças que podem levar à sua destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada.

"O capital humano, que abrange as capacidades individuais, conhecimentos, habilidades e experiências dos empregados de uma empresa, aliado ao capital estrutural constituem o capital intelectual das organizações". (WEBER; ROCHA; NASCIMENTO, 2001, p. 74).

É inquestionável o valor das informações, tanto para as empresas quanto para as pessoas que as utilizam, sendo a informação, às vezes, tida como o bem mais valioso que uma empresa pode ter.

Conforme Fontes (2006, p. 2), você pode não ter se dado conta, mas "a informação é um recurso que move o mundo, além de nos dar conhecimento de como o universo está caminhando". Prestando atenção, podemos identificar que somos o que somos porque transformamos informação em vida.

2.1 ETAPAS DO CICLO DE VIDA DA INFORMAÇÃO

FIGURA 1 – FLUXO DA INFORMAÇÃO EM UMA ORGANIZAÇÃO

FONTE: Beal (2008, p. 4)

O ciclo de vida da informação, de acordo com Sêmola (2003, p. 9), "é composto e identificado pelos momentos vividos pela informação que a colocam em risco". Tais momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da organização.

A informação utilizada pela organização é um bem valioso e precisa ser protegido e gerenciado. (SÊMOLA, 2003, p. 19).

2.1.1 Identificação das necessidades e dos requisitos

Segundo Beal (2008, p. 5), "identificar as necessidades de informação dos grupos e indivíduos que integram a organização e de seus públicos externos é um passo fundamental para que possam ser desenvolvidos serviços e produtos informacionais orientados especificamente para cada grupo e necessidade interna e externa". O esforço de descoberta das necessidades e dos requisitos de informação é recompensado quando a informação se torna mais útil e os seus destinatários, mais receptivos a aplicá-la na melhoria de produtos e processos (usuários internos) ou no fortalecimento dos vínculos e relacionamentos com a organização (usuários externos).

2.1.2 Obtenção

Definidas as necessidades de informação, conforme Beal (2008, p. 5), a próxima etapa é a de obtenção das informações que podem suprir essas necessidades. Nesta etapa, "são desenvolvidas as atividades de criação, recepção ou captura de informação, proveniente de fonte externa ou interna, em qualquer mídia ou formato". Na maioria dos casos, o processo de obtenção da informação não é pontual, precisando repetir-se ininterruptamente para alimentar os processos organizacionais (por exemplo, informações sobre o grau de satisfação de clientes com os produtos ofertados normalmente serão coletados repetidamente, por meio de pesquisas periódicas).

Uma preocupação típica da etapa de obtenção diz respeito à *integridade da informação*: "é preciso garantir que a informação é genuína, criada por alguém autorizado a produzi-la (ou proveniente de uma fonte confiável), livre de adulteração, completa e apresentada dentro de um nível de precisão compatível com os requisitos levantados na etapa de identificação das necessidades". (BEAL, 2008, p. 5).

2.1.3 Tratamento

Antes de estar em condições de ser aproveitada, de acordo com Beal (2008, p. 5-6), "é comum que a informação precise passar por processos de organização, formatação, estruturação, classificação, análise, síntese, apresentação e reprodução, para torná-la mais acessível, organizada e fácil de localizar pelos usuários". Nesta etapa, a preocupação com a *integridade* continua em evidência, principalmente se estiverem envolvidas técnicas de adequação do estilo e adaptação de linguagem, contextualização e condensação da informação, entre outras. O uso dessas técnicas deve levar em conta a preservação das características de quantidade e qualidade necessárias para que a informação efetivamente sirva ao fim a que se propõe. No caso das atividades de reprodução da informação para posterior distribuição, as questões relacionadas à preservação da confidencialidade podem adquirir grande relevância, uma vez que a existência de diversas cópias de uma mesma informação, qualquer que seja a mídia utilizada (computador, papel, disquete, fita de áudio ou vídeo etc.), amplia os problemas de restrição de acesso aos usuários devidamente autorizados.

2.1.4 Distribuição / transporte

Sêmola (2003, p. 10) cita que o transporte "é o momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico (*e-mail*), ao postar um documento via aparelho de fax, ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo".

Segundo Beal (2008), a etapa de distribuição da informação permite levar a informação necessária a quem precisa dela. Quanto melhor a rede de comunicação da organização, mais eficiente é a distribuição interna da informação, o que aumenta a probabilidade de que esta venha a ser usada para apoiar processos e decisões e melhorar o desempenho corporativo. É necessário considerar, nesta etapa, "os diversos objetivos de segurança da comunicação, devendo ser analisados separadamente os requisitos de segurança relacionados aos processos de distribuição interna de informação daqueles voltados para a disseminação para públicos externos (parceiros, fornecedores, clientes, acionistas, grupos de pressão, governo etc.)". (BEAL, 2008, p. 6).

2.1.5 Uso

Beal (2008) cita que o uso é a etapa mais importante de todo o processo de gestão da informação, embora seja frequentemente ignorado nos processos de gestão das organizações. Não é a existência da informação que garante os melhores resultados numa organização, mas sim o uso, dentro de suas finalidades básicas: conhecimento dos ambientes interno e externo da organização e atuação nesses ambientes. Nesta etapa, os objetivos de *integridade* e *disponibilidade* devem receber atenção especial: uma informação deturpada, difícil de localizar ou indisponível pode prejudicar as decisões e operações da organização. Como já mencionado, a preocupação com o uso legítimo da informação pode levar a requisitos de *confidencialidade*, destinados a restringir o acesso e o uso de dados e informações às pessoas devidamente autorizadas.

2.1.6 Armazenamento

Segundo Sêmola (2003, p. 10), "o armazenamento é o momento em que a informação é armazenada, seja em banco de dados compartilhado, em anotação de papel posteriormente postada em um arquivo de ferro, ou, ainda, em mídia de disquete depositada na gaveta da mesa de trabalho".

Conforme Beal (2008, p. 6-7), a etapa de armazenamento é necessária para assegurar a conservação dos dados e informações, permitindo seu uso e reuso dentro da organização. Nesta etapa, "os objetivos de *integridade* e *disponibilidade* dos dados e informações armazenados podem adquirir maior destaque. A complexidade da conservação dos dados obviamente aumenta à medida que cresce a variedade de mídias usadas para armazená-los: bases de dados informatizadas, arquivos magnéticos ou ópticos, documentos em papel etc.". A necessidade de se precaver contra problemas na recuperação dos dados pode exigir a migração periódica dos acervos digitais para tecnologias mais atualizadas, para protegê-los de mudanças nos métodos de gravação, armazenamento e recuperação, que ocorrem a ciclos cada vez menores devido aos constantes avanços nas tecnologias da informação e comunicação.

Toda informação deve ser protegida contra desastres físicos (fogo, calor, inundação etc.) e lógicos (vírus, acesso indevido, erro de programas, alteração incorreta etc.). (SÊMOLA, 2003, p. 58).

Mesmo com o desenvolvimento de mídias mais estáveis, com expectativa de vida útil superior às mídias magnéticas, tais como CD-ROM e DVD, a recuperação dos documentos ficaria inviável se não houvesse no futuro dispositivos capazes de ler essas mídias; o processo de migração periódica visa evitar esse problema. No caso de dados sigilosos, é necessário considerar os tipos de mecanismo de proteção a serem usados para impedir o acesso físico ou remoto por pessoas não autorizadas.

O acesso à informação somente deve ser feito se o usuário estiver previamente autorizado. (SÊMOLA, 2003, p. 44).

2.1.7 Descarte

De acordo com Sêmola (2003, p. 10), "o descarte é o momento no qual a informação é descartada, seja ao depositar um material impresso na lixeira da empresa, ao excluir um arquivo eletrônico de seu computador, ou ainda, ao descartar uma mídia usada que apresentou erro na sua leitura".

Quando uma informação se torna obsoleta ou perde a utilidade para a organização, ela deve ser objeto de processos de descarte que obedeçam a normas legais, políticas operacionais e exigências internas. Excluir dos repositórios de informação corporativos os dados e as informações inúteis melhora o processo de gestão da informação de diversas formas: economizando recursos de armazenamento, aumentando a rapidez e eficiência na localização da informação necessária, melhorando a visibilidade dos recursos informacionais importantes etc. Entretanto, o descarte de dados e informações precisa ser realizado dentro de condições de segurança, principalmente no que tange ao aspecto da *confidencialidade*, e, em menor grau, também de *disponibilidade*. No que tange à confidencialidade, o descarte de documentos e mídias que contenham dados de caráter sigiloso precisa ser realizado com observância de critérios rígidos de destruição segura (por exemplo, o uso de máquinas fragmentadoras para documentos em papel, ou de *softwares* destinados a apagar com segurança arquivos de um microcomputador que, se simplesmente excluídos do sistema, poderiam ser facilmente recuperados com o uso de ferramentas de restauração de dados). Do ponto de vista da disponibilidade, as preocupações incluem a legalidade da destruição de informações que podem vir a ser exigidas no futuro e a necessidade de preservar dados históricos valiosos para o negócio, entre outras. (BEAL, 2008).

Conforme Beal (2008, p. 7-8),

a descoberta de informações sigilosas ou dados pessoais sujeitos a normas de privacidade em computadores usados quando estes são transferidos de área, doados ou vendidos durante um processo de renovação do parque de computadores da organização é relativamente comum. A existência e o cumprimento de procedimentos formais de descarte de computadores e mídias de armazenamento podem evitar constrangimentos e prejuízos à imagem e credibilidade da organização, permitindo que os itens descartados sejam auditados e tenham os seus dados apagados de maneira segura antes destes serem transferidos para os seus novos proprietários.

2.2 SEGURANÇA DA INFORMAÇÃO BASEADA EM TI

Grande parte das informações e dos dados importantes para as organizações é, segundo Beal (2008), armazenada em computadores. As organizações dependem da fidedignidade da informação fornecida pelos seus sistemas baseados em TI, e se a confiança nestes dados for destruída, o impacto poderá ser comparado à própria destruição destes sistemas.

TI, ou Tecnologia da Informação, de acordo com Beal (2008, p. 8), "é uma solução ou um conjunto de soluções sistematizadas baseadas em métodos, recursos de informática, comunicação e multimídia, que tem por objetivo resolver os problemas relativos a gerar, tratar, processar, armazenar, veicular e reproduzir dados, e ainda subsidiar os processos que convertam estes dados em informações".

De acordo com Baltzan e Phillips (2011, p. 9), "a TI dedica-se ao uso da tecnologia na gestão e processamento da informação, podendo a tecnologia da informação ser um facilitador considerável do sucesso das organizações e da inovação em seus negócios".

A tecnologia da informação, segundo Laudon e Laudon (2004, p. 13), "é uma das diversas ferramentas que os gestores usam para enfrentar mudanças".

De acordo com Beal (2008, p. 8), entende-se por informação baseada em Tecnologia da Informação, a informação residente em base de dados, arquivos informatizados, mídias magnéticas ou outras que exijam soluções de informática para acessá-las. A direção das organizações deve preocupar-se com a segurança dos componentes de TI e da informação neles armazenada por quatro razões principais:

- Dependência da tecnologia da informação: sistemas que oferecem serviços adequados no tempo certo são a chave para a sobrevivência da maioria das organizações. Sem seus computadores e sistemas de comunicação, as organizações são incapazes de fornecer seus serviços, contratar

fornecedores e clientes, processar faturas ou efetuar pagamentos. Os sistemas de informação também armazenam dados sigilosos que, se publicados, podem causar prejuízos e, em alguns casos, o fracasso destas organizações.

- Vulnerabilidade da infraestrutura tecnológica: *hardware* e *software* exigem ambientes estáveis e podem ser danificados por catástrofes e desastres naturais, como incêndios, alagamentos, inundações, terremotos, falhas no controle da temperatura ambiental ou do fornecimento de energia elétrica, sabotagens ou acidentes. Diversos equipamentos de TI são alvos de ladrões tendo em vista a sua portabilidade ou devido ao fato de apresentarem uma relação entre custo e peso bastante elevada, sendo facilmente comercializados.
- Alto valor das informações armazenadas: os sistemas baseados em TI são a chave para o acesso a grandes quantidades de dados corporativos, tornando-se um alvo atraente para *hackers*, espiões e até mesmo alguns empregados dispostos a abusar de seus privilégios em troca de dinheiro ou algum tipo de vantagem oferecida por algum concorrente.
- Pouca atenção dada à segurança nos estágios iniciais do desenvolvimento de *software*: muitos sistemas de informação, sejam eles desenvolvidos internamente, sejam adquiridos de terceiros, não foram projetados considerando a segurança das informações como uma de suas prioridades. É comum que algumas características de segurança (por exemplo, as relacionadas à definição de níveis de permissão de acesso a funcionalidades, segregação de atividades no sistema, e outras mais) sejam adicionadas nas etapas finais de desenvolvimento, quando a sua eficácia já pode ter sido prejudicada por decisões de projeto tomadas sem levar em conta os requisitos de segurança.

De acordo com Beal (2008, p. 9), "o termo *hacker* serve para referenciar indivíduos que buscam obter acesso não autorizado a sistemas computacionais com o propósito de acessar informações, corromper dados ou utilizar os recursos disponíveis para realizar atividades ilegítimas numa rede".

Conforme Baltzan e Phillips (2012, p. 114), "*hackers* são extremos conhecedores de computadores que usam seu conhecimento para invadir os computadores de outras pessoas".

Stair e Reynolds (2001, p. 543) comentam que "um *hacker*, também chamado cracker, é uma pessoa habilidosa no uso do computador que tenta obter acesso não autorizado ou ilegal aos sistemas computacionais para roubar senhas, corromper arquivos e programas ou mesmo para transferir dinheiro. Em muitos casos, os *hackers* são pessoas que buscam agito – o desafio de vencer o sistema".

Segundo Laudon e Laudon (2004, p. 170), "*hackers* exploram os pontos fracos da segurança da Web para obter acesso a dados como informações sobre clientes e senhas. Podem usar 'cavalos de Troia' (Trojan), *softwares* que se passam por legítimos, para obter informações de um computador hospedeiro".

2.3 SEGURANÇA DA INFORMAÇÃO NÃO ARMAZENADA EM TI

Ainda que seja fundamental garantir confidencialidade, integridade e disponibilidade das informações importantes para o negócio, a segurança da informação baseada em TI não resolve todas as ameaças a que se sujeita a informação corporativa. Existem inúmeras razões, segundo Beal (2008, p. 9), para também proteger informações não armazenadas em computadores:

- Toda organização possui dados, informações e conhecimentos valiosos que não estão armazenados em sistemas informatizados ou meios eletrônicos, seja por falta de tempo ou interesse do detentor da informação de registrá-la, ou ainda por estar temporariamente disponível apenas em um documento impresso, microfilme ou outro tipo de meio de registro e suporte da informação.
- Alguns documentos têm sua validade vinculada ao suporte físico em papel, exigindo proteção física mesmo existindo cópias eletrônicas destes.
- Informações armazenadas em computadores podem ser impressas e ter sua confidencialidade comprometida pela falha no manuseio de suas versões impressas.

Os processos de segurança da informação devem levar em conta as questões relativas à segurança da informação armazenada em meios não eletrônicos para garantir uma proteção adequada para dados e informações importantes para o negócio. Ter uma noção clara de quais informações valiosas permanecem armazenadas fora dos componentes de TI, bem como dos fluxos por elas percorridos na organização, permite aos responsáveis pela preservação desses ativos planejar e implementar as medidas necessárias para sua proteção (BEAL, 2008).

2.4 PROTEÇÃO DOS ATIVOS INFORMACIONAIS

A fim de manter os ativos de informação protegidos contra perda, furto e alteração, divulgação ou destruição indevida, além de outros problemas que podem afetá-los, as organizações precisam adotar controles de segurança – medidas de proteção que abrangem, de acordo com Beal (2008, p. 10), "uma grande diversidade de iniciativas, indo dos cuidados com os processos de comunicação à segurança de pessoas, mídias e componentes de TI".

Ainda conforme Beal (2008, p. 10), "os controles de segurança precisam ser escolhidos levando-se em conta os riscos reais a que estão sujeitos os dados, informações e conhecimentos gerados pelas organizações, para serem capazes de protegê-los adequadamente". Toda organização deve adquirir uma visão sistêmica de suas necessidades de segurança, dos recursos que devem ser protegidos e das ameaças às quais está sujeita, para poder identificar as mais adequadas medidas

de proteção, viáveis economicamente e capazes de minimizar ou eliminar os principais riscos para o negócio.

3 RISCOS ENVOLVENDO INFORMAÇÕES

Apesar de a segurança ser, de acordo com Nakamura e Geus (2007, p. 51), essencial para os negócios das organizações, a dificuldade em entender sua importância ainda é muito grande. Muitas vezes, a única segurança existente é a obscuridade, e esta obscuridade constitui um risco muito grande para a organização, pois, cedo ou tarde, alguém poderá descobrir que um grande tesouro está à sua total disposição.

De acordo com Beal (2008, p. 12), "risco é a combinação da probabilidade de um evento e sua consequência".

Já conforme Ferreira e Araújo (2008, p. 163), "risco trata-se de um possível evento/ação que, se efetivado, gera um impacto negativo, em função da exploração da fraqueza/vulnerabilidade, considerando tanto a probabilidade quanto o impacto de ocorrência".

Por fim, segundo Sêmola (2003, p. 50), "risco é a probabilidade de algumas ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios".

Tendo em vista a complexidade e o alto custo de manter os ativos de informação a salvo de ameaças à sua confidencialidade, integridade e disponibilidade, "é de extrema importância para o alcance dos objetivos de segurança adotar um enfoque de gestão baseado nos riscos específicos para o negócio", segundo Beal (2008, p. 11). Conhecendo as ameaças e vulnerabilidades a que estão sujeitas as informações, bem como os impactos que poderiam advir do comprometimento de sua segurança, torna-se mais bem fundamentada e confiável a tomada de decisão sobre como e quanto gastar com a proteção dos dados corporativos.

> A constante avaliação de riscos de T.I. e de ativos críticos de informação na organização irá permitir uma evolução constante e um aprimoramento em termos de controles mais eficazes, inteligentes, com custos adequados e alinhados ao apetite de riscos da empresa. O circulo virtuoso é composto por uma avaliação de riscos, análise de resultados da avaliação, reporte dos pontos levantados, aplicação de melhorias e reinício do ciclo. A cada rodada da avaliação de riscos, mais o processo vai sendo refinado e maior a confiabilidade nos controles e na sua eficiência e adequação. (FERREIRA; ARAÚJO, 2008, p. 195).

3.1 RISCOS NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

Beal (2008, p. 13) cita que os termos e definições do ISO Guide 73, "norma que estabelece um vocabulário de dezenas de termos relacionados à gestão de riscos, dizem respeito a todo e qualquer tipo de situação (ou evento) que constitui oportunidade de favorecer ou prejudicar o sucesso de um empreendimento". Em sua introdução, a norma alerta para o fato de que o objetivo do documento é prover um vocabulário básico para desenvolver um entendimento comum a organizações de diversos países, sendo possível que eventuais adaptações precisem ser realizadas nas expressões utilizadas para atender às necessidades dentro de um domínio específico.

No setor financeiro, por exemplo, a gestão do risco está associada a flutuações monetárias representadas tanto por oportunidades de ganho quanto de perda, e consequentemente o processo de gestão de risco trabalha igualmente com os aspectos negativos e positivos da situação de risco.

> Em outras áreas, como a de prevenção de acidentes, a gestão do risco tem a preocupação de prevenir e evitar impactos negativos associados aos acidentes. Diante de tantos cenários diferentes de aplicação da gestão do risco, é importante promover ajustes na terminologia adotada, alterando-a e expandindo-a na medida do necessário para tratar a questão dentro do escopo em que está sendo estudada a gestão do risco. (BEAL, 2008, p. 14).

Cada negócio, de acordo com Sêmola (2003, p. 55), "independente de seu segmento de mercado e seu *core business*, possui dezenas, talvez centenas, de variáveis que se relacionam direta e indiretamente com a definição do seu nível de risco. Identificar estas variáveis passa a ser a primeira etapa do trabalho".

De acordo com Sêmola (2003, p. 55-56), "O risco é a probabilidade de que agentes, que são ameaças, explorem vulnerabilidades, expondo os ativos a perdas de confidencialidade, integridade e disponibilidade, e causando impactos nos negócios. Esses impactos são limitados por medidas de segurança que protegem os ativos, impedindo que as ameaças explorem as vulnerabilidades, diminuindo, assim, o risco".

$$R = \frac{V \times A \times I}{M}$$

Segundo Sêmola (2003, p. 56),

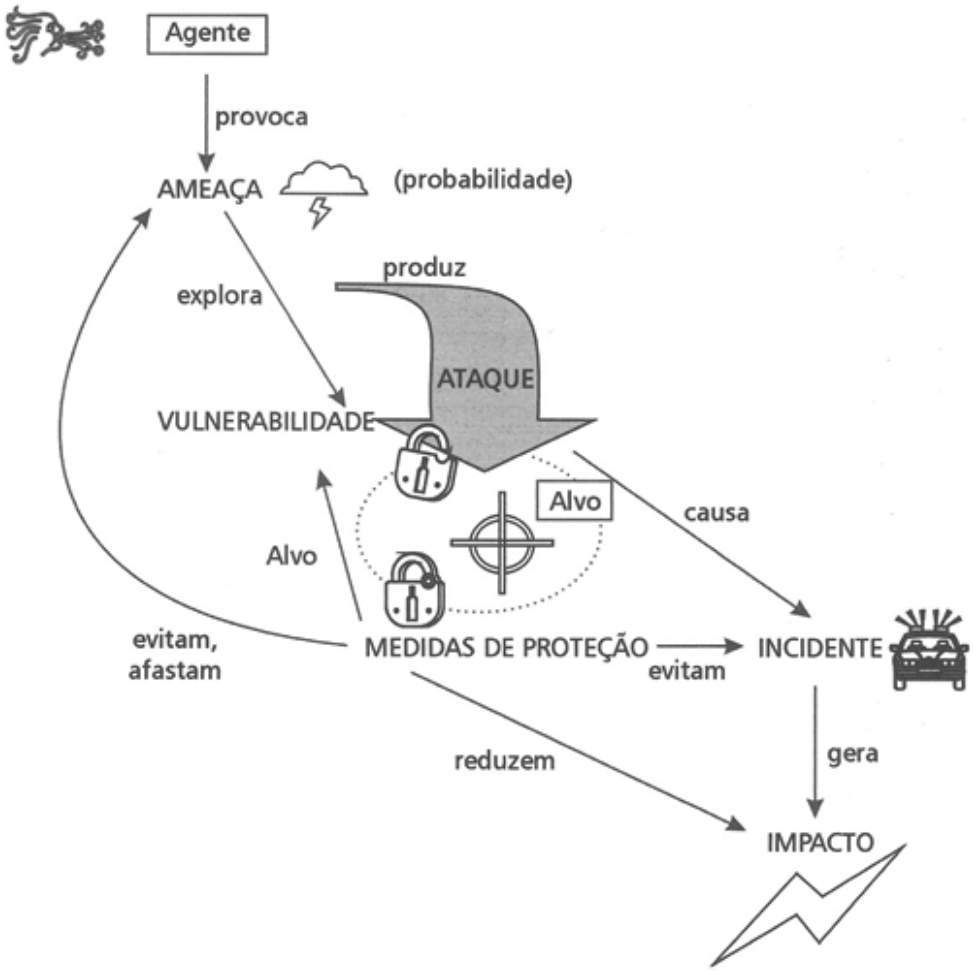
> por melhor que estejam protegidos os ativos, novas tecnologias, mudanças organizacionais e novos processos de negócio podem criar vulnerabilidades ou identificar e chamar a atenção para as já existentes. Além disso, novas ameaças podem surgir e aumentar significativamente a possibilidade de impactos no negócio. Sendo assim, medidas corretivas de segurança precisam ser consideradas, pois sempre haverá a possibilidade de um incidente ocorrer, por mais que tenhamos tomado todas as medidas preventivas adequadas.

É fundamental, ainda conforme Sêmola (2003, p. 56),

> que todos tenhamos a consciência de que não existe segurança total e, por isso, devemos estar bem estruturados para suportar mudanças nas variáveis da equação, reagindo com velocidade e ajustando o risco novamente aos padrões pré-especificados como ideal para o negócio.

Diante disso, concluímos que não há um resultado R (risco) igual para todos. Sempre será necessário avaliar o nível de segurança apropriado para cada momento vivido pela empresa, como se tivéssemos de nos pesar em períodos regulares para definir a melhor dose de ingestão calórica (dose de segurança) do período, a fim de buscar aproximação com o peso ideal (nível de risco) para o momento (SÊMOLA, 2003).

FIGURA 2 – RELAÇÃO ENTRE OS TERMOS ASSOCIADOS AO RISCO PARA SEGURANÇA DA INFORMAÇÃO

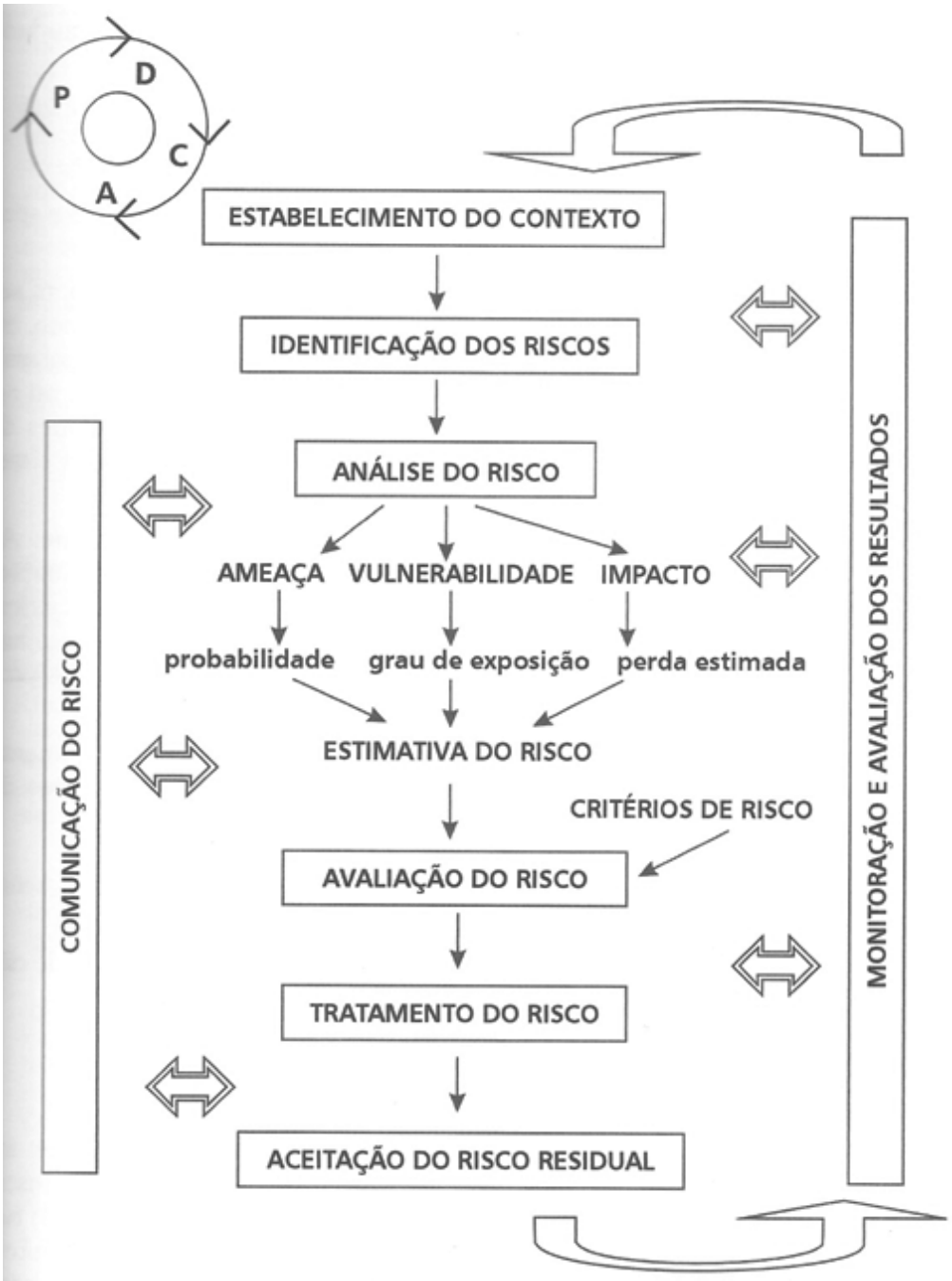


FONTE: Beal (2008, p. 16)

3.2 ETAPAS DA GESTÃO DO RISCO

A administração do risco, de acordo com Beal (2008, p. 16), "precisa contemplar várias etapas cíclicas que levam à redução do risco, indo da análise ao tratamento, aceitação e comunicação". A figura a seguir é útil para fornecer uma visualização global desses processos.

FIGURA 3 – ETAPAS DA GESTÃO DO RISCO



FONTE: Beal (2008, p. 17)

No topo à esquerda da Figura 3, há a representação do ciclo PDCA, que permite entender a gestão da segurança da informação como um ciclo contínuo de planejamento, execução, avaliação e ação corretiva. O PDCA (de *plan*, *do*, *check*, *act*), método utilizado em processos de gestão da qualidade que se aplica aos mais diversos tipos e níveis de gestão, conforme Beal (2008, p. 37), "é útil para fornecer uma visualização global das etapas que devem compor a gestão da segurança da informação".

O significado da sigla PDCA, conforme Beal (2008, p. 37), vem de:

- P = *Plan*, de planejar: estabelecer objetivos metas e meios de alcançá-los.
- D = *Do*, de executar.
- C = *Check*, de verificar, avaliar (comparação do resultado com o planejado).
- A = *Act*, de agir corretivamente (caso sejam detectados desvios ou falhas a serem corrigidos).

3.3 ANÁLISE E AVALIAÇÃO DO RISCO

O processo de gestão do risco, segundo Beal (2008, p. 18), "inicia-se com a identificação dos riscos e seus elementos: alvos, agentes, ameaças, vulnerabilidades, impactos".

As ameaças a que se sujeitam informação e ativos de informação podem ser classificadas como ambientais (naturais, como fogo, chuva, raio, terremoto, ou decorrentes de condições do ambiente, como interferência eletrônica, contaminação por produtos químicos, falhas no suprimento de energia elétrica ou no sistema de climatização), técnicas (configuração incorreta de componentes de TI, falhas de *hardware* e *software*), lógicas (códigos maliciosos, invasão de sistema) e humanas (erro de operação, fraude, sabotagem) (BEAL, 2008).

Conforme Beal (2008, p. 18), "ameaças exploram vulnerabilidades para atingir alvos de ataque. As vulnerabilidades determinam o grau de exposição de um ativo de informação, ambiente ou sistema a determinada ameaça". A falta de treinamento dos usuários, por exemplo, representa uma vulnerabilidade em relação à ameaça de erro humano, assim como a instalação de um *data center* no subsolo de um prédio produz uma vulnerabilidade associada à ameaça de inundação.

Vulnerabilidades lógicas observadas em sistemas conectados à internet incluem senhas de administrador vindas de fábrica que não são alteradas na instalação do *software*, ausência de instalações de *patches* após a descoberta de um *bug* no sistema e permanência de utilitários e ferramentas de administração que tornam o computador inseguro e não são necessários para o seu funcionamento no dia a dia. *Hackers* dispõem de várias técnicas para descobrir vulnerabilidades dessa natureza e, com esse conhecimento, planejar um ataque.

QUADRO 1 – RELAÇÃO DE AMEAÇAS E IMPACTOS RELACIONADOS A INSTALAÇÕES E COMPONENTES DE TI

Ameaça	**Tipo de recurso vulnerável (alvo)**	**Impacto para o objetivo de confidencialidade**	**Impacto para o objetivo de integridade**	**Impacto para o objetivo de confidencialidade**
Desastres naturais como terremoto, nevasca e furacão.	Edifícios, torres de comunicação.	Controles físicos de acesso podem ser desconsiderados durante a recuperação do desastre e equipamentos descartados podem conter informações confidenciais.		Todos os serviços podem ser prejudicados e dados podem ser perdidos ou permanecerem temporariamente indisponíveis.
Falhas ambientais, incluindo queda da energia elétrica.	*Hardware.*			Serviços podem ser interrompidos e *hardware* pode ser danificado.
Furto	Equipamentos valiosos e portáteis.	Equipamentos furtados podem conter informações confidenciais.		Serviços podem ser interrompidos e dados podem ser perdidos.
Vírus.	Principalmente computadores pessoais conectados em rede.		Dados podem ser corrompidos pelo vírus.	Computadores infectados podem parar de funcionar e dados importantes podem ser apagados.
Hacking.	Todos os sistemas em rede.	O objetivo dos *hackers* pode ser a quebra do sigilo de informações ou a indisponibilidade dos serviços (ataque do tipo *DoS*, *Denial of Service*), a alteração ou destruição de dados ou a utilização dos recursos informatizados da organização para realizar invasões a terceiros.		
Código escondido.	Todo o *software.*	Código não autorizado pode levar ao vazamento de informações sigilosas tais como senhas de acesso.	Funções escondidas podem manipular dados indevidamente.	Programas podem ser projetados para destruir dados ou negar acesso autorizado a serviços.

Falha de *hardware*.	Todo o *hardware*	*Hardware* danificado pode ser enviado para manutenção contendo informação sigilosa.	Dados podem ser corrompidos quando o *hardware* falha.	Serviço indisponível.
Falha de *software*	Todo o *software*.	A falha dos controles de acesso pode levar à divulgação indevida de dados e informações	Dados podem ser corrompidos.	Serviço indisponível.
Erro Humano.	Todos os sistemas.	Funcionários podem divulgar acidentalmente informações sigilosas, por exemplo, enviando dados para a impressora errada.	Funcionários podem inserir dados incorretamente.	Funcionários podem destruir informações acidentalmente, danificar *hardware* ou interromper o funcionamento do sistema por erro de configuração.

FONTE: Adaptado de Beal (2008, p. 20-21)

A figura 3 demonstra como a decomposição do risco em seus componentes e a posterior avaliação das "características mensuráveis" desses componentes levam a uma estimativa do valor do risco, que depois poderá ser comparado a uma referência (critério do risco) para determinar sua relevância, permitindo tomar a decisão de aceitar ou tratar este risco. Várias são as metodologias desenvolvidas para realizar a análise e avaliação de riscos, sendo estas usualmente classificadas como qualitativas e quantitativas.

Os métodos quantitativos de avaliação do risco são particularmente úteis quando se tenta buscar um equilíbrio entre os custos de implementação de medidas de segurança e o possível custo da não implementação dessa segurança. Um dos métodos quantitativos mais conhecidos é o de cálculo da Expectativa de Perda Anual (ALE, do inglês *Annual Loss Expectation*). A ALE é calculada pela multiplicação da perda prevista para um incidente pela frequência esperada de ocorrência desse incidente. A metodologia fundamenta-se no princípio de que durante um período de 12 meses *n* incidentes irão ocorrer para cada tipo de ameaça (*n* pode ser uma fração, nos casos de incidentes menos frequentes). Se cada incidente resulta numa perda média de *i*, então a ALE será o produto dos dois, *n x i*. Por meio desse método é possível tomar decisões em relação a investimentos em segurança: medidas de proteção com um custo anual de *X* seriam justificadas se sua implantação significasse uma expectativa de redução da ALE maior que *X* (BEAL, 2008).

Os métodos quantitativos costumam ser vistos com cautela pelos estudiosos, conforme Beal (2008, p. 22),

> devido à dificuldade de obtenção de resultados representativos (é preciso dispor de um histórico confiável dos incidentes de segurança passados e dos impactos financeiros a eles associados para garantir resultados representativos, e mesmo que o histórico esteja disponível, as condições podem ter mudado, tornando os dados pouco confiáveis).

A necessidade de medir os impactos em termos monetários também nem sempre é uma expectativa realista. Por exemplo, quando se analisa a expectativa de perda anual associada à interrupção do serviço de um *site* de comércio eletrônico, mesmo que seja possível calcular uma média do tempo previsto até a recuperação do serviço e a perda da receita a ela associada, como garantir que o impacto financeiro causado resuma-se à perda imediata de receita? Muitos clientes poderiam ficar insatisfeitos e mudar de fornecedor após sofrerem uma ou mais falhas de serviço, e dificilmente seria possível estimar de forma confiável essa perda para acrescentá-la ao cálculo da ALE, principalmente se as condições externas tiverem se alterado (por exemplo, com a recente entrada no mercado de concorrentes poderosos).

Apesar dessas dificuldades, Schneier (2000 apud BEAL, 2008, p. 22) considera esse tipo de análise importante para dar perspectiva às questões de segurança: grandes falhas de segurança serão aceitáveis se a probabilidade de ataque em relação a elas estiver perto de zero; já pequenas falhas podem ter que ser eliminadas se forem objeto de 10 milhões de ataques por dia. O autor ilustra esse ponto comparando duas situações:

- O risco de espionagem por um concorrente interessado em roubar os novos planos de *design* da empresa pode ter uma perda associada de US$ 10 milhões, mas se a frequência estimada de ocorrência for de, por exemplo, 0,001 (0,1% de probabilidade de ocorrência), o ALE cai para US$ 10 mil, desestimulando grandes investimentos em minimizar este risco.
- A perda esperada para um incidente de invasão por *hackers* pode ser de apenas US$ 10 mil (custo estimado de contratar alguém para identificar e corrigir o problema e outras despesas envolvidas), mas se a frequência de ocorrência for alta – por exemplo, 3 vezes por dia, ou 1.000 por ano –, a ALE seria de US$ 10 milhões, suficiente para justificar, por exemplo, a implantação de um *firewall* de US$ 25 mil para proteger a rede.

De acordo com Beal (2008, p. 23), "os métodos qualitativos trabalham com a descrição literal dos riscos para avaliá-los". Diversos métodos para avaliação qualitativa de riscos utilizam questionários e matrizes de riscos como o apresentado no quadro a seguir.

QUADRO 2 – EXEMPLO DE UMA MATRIZ DE RISCOS

Gravidade do impacto	**Probabilidade de ocorrência do incidente**					
	F Impossível	**E Improvável**	**D Remota**	**C Ocasional**	**B Provável**	**A Frequente**
I Catástrofe			/////////	XXXXXX	XXXXXX	XXXXXX
II Alta				/////////	XXXXXX	XXXXXX
III Média					/////////	/////////
IV Baixa						
Legenda	XXXXXX: Imperativo reduzir os riscos. /////////: Medidas de proteção adicionais requeridas. Em branco: As medidas básicas de proteção adotadas pela organização são consideradas suficientes para manter os riscos em níveis aceitáveis.					

FONTE: Adaptado de Beal (2008, p. 23)

No exemplo do Quadro 2, a possibilidade de um incidente apresenta seis níveis, estimada de acordo com a frequência esperada da ocorrência ao longo de um período de tempo ou no grau de confiança na ocorrência do incidente. Já a gravidade do impacto pode ser classificada como catastrófica quando o dano representa o fracasso da organização, a baixa quando um ataque bem-sucedido não é capaz

de provocar efeitos adversos consideráveis. A matriz resultante da combinação dessas duas dimensões, confrontada com critérios de risco previamente definidos, leva à identificação dos riscos que necessariamente têm que ser reduzidos (neste exemplo pertencentes às células marcadas com XXXXXX e ///////// no quadro) pelo uso de medidas de proteção complementares aos controles básicos adotados pela organização.

De acordo com Beal (2008), um gerente de segurança encarregado de um projeto de avaliação de riscos normalmente terá dificuldade em identificar o melhor método para realizar uma análise de risco, e mesmo em optar pelo uso de um método quantitativo ou qualitativo específico dentre as diversas abordagens ofertadas no mercado. Normalmente, os métodos de avaliação do risco costumam ter um foco específico como tecnológico, ambiental etc. Muitas vezes uma avaliação de risco completa irá exigir a combinação de diferentes métodos avaliativos para garantir uma análise abrangente do ambiente físico e lógico a ser protegido.

Ainda conforme Beal (2008), os métodos quantitativos são aconselháveis sempre quando é cogitada a adoção de uma medida de proteção de alto custo para a organização. Nesse caso, uma estimativa de perda esperada pode ser comparada com o custo da solução escolhida, a fim de que se possa chegar a uma conclusão a respeito da razoabilidade do investimento proposto para reduzir o risco. Já o uso de métodos qualitativos pode beneficiar as organizações que não dispõem de recursos financeiros, tecnológicos e de pessoal para realizar uma avaliação de risco muito sofisticada. Uma análise simplificada pode ser desenvolvida mediante a classificação do risco com base em critérios objetivos previamente estabelecidos para as principais ameaças identificadas, conforme exemplificado no quadro a seguir.

QUADRO 3 – EXEMPLOS DE CRITÉRIOS SIMPLIFICADOS PARA PONTUAÇÃO DOS PRINCIPAIS RISCOS DE SEGURANÇA

Risco de incidentes naturais: desastres causados por fogo, inundação, terremoto, furacão.	0 pontos: baixo risco. As instalações estão situadas em local seguro, protegido contra incêndio. Não há histórico de inundação, terremoto e furacão na área.
	4 pontos: alto risco. As instalações apresentam problemas na rede elétrica e não possuem dispositivos de segurança contra incêndio. Os principais recursos estão no subsolo e correm risco quando há muita chuva.
Risco de falhas ambientais como temperatura excessiva e queda de energia elétrica.	0 pontos: baixo risco. A organização está dotada de equipamentos *no-break*, geradores e ar-condicionado, e não existe histórico de falhas ambientais.
	4 pontos: alto risco. Problemas com a rede elétrica e outras falhas ambientais têm-se mostrado frequentes e com sérias consequências para a disponibilidade dos sistemas.
Risco de furto.	0 pontos: baixo risco. Não existem equipamentos portáteis do tipo notebook, e a segurança interna é bastante rígida, não havendo histórico de furto de equipamentos ou componentes.
	4 pontos: alto risco. O acesso de estranhos não é controlado, os funcionários utilizam *notebooks* em viagens, ou já foram registradas ocorrências de furto ou perda de equipamento.

FONTE: Adaptado de Beal (2008, p. 25)

Os processos de análise e avaliação do risco incluem, quase sempre, tarefas de reunião extensiva de dados, agrupamento, computação e relatório. Existem variadas metodologias e ferramentas disponíveis comercialmente que reduzem significativamente o esforço de cálculo e de documentação, e podem ser indispensáveis para uma avaliação de risco detalhada e abrangente, devido ao grande volume de dados a ser coletado, armazenado, processado e documentado. Apesar de úteis, esses recursos não substituem pessoal qualificado e experiente, e, portanto, não oferecem soluções em si mesmos, apenas uma estrutura na qual basear o trabalho (BEAL, 2008).

Conforme Nakamura e Geus (2007, p. 59-60), alguns dos riscos existentes e algumas considerações a serem feitas são:

- A falta de uma classificação das informações e dimensionamento quanto ao seu valor e à sua confiabilidade, que serve de base para a definição de uma estratégia de segurança adequada. Isso resulta em um fator de risco para a organização, além de dificultar o dimensionamento das perdas resultantes de um ataque.
- O controle de acesso mal definido faz com que os usuários tenham acesso irrestrito a quaisquer partes do sistema, mesmo as que não são necessárias para a realização de suas tarefas.
- Autenticação com base em identidades compartilhadas, como o uso de usuários e senhas únicas, faz com que não seja possível identificar a origem de acessos não autorizados.
- A dificuldade de controle do administrador sobre todos os sistemas da rede interna faz com que estes não possam ser considerados confiáveis. Os '*bugs*' nos sistemas operacionais ou nos *softwares* utilizados por estes equipamentos podem abrir 'brechas' na rede interna.
- A internet deve ser considerada um ambiente hostil e, portanto, não confiável. Assim, todos os seus usuários devem ser considerados não confiáveis e atacantes em p.
- As informações e senhas que trafegam pela rede estão sujeitas a serem capturadas.
- Os *e-mails* podem ser capturados, lidos, modificados e falsificados.
- Qualquer conexão entre a rede interna e qualquer outro ponto pode ser utilizada para ataques à rede interna.
- Os telefones podem ser grampeados e as informações que trafegam pela linha, sejam por voz ou dados, gravadas.
- Um atacante precisa encontrar somente uma brecha para realizar um ataque, enquanto o gestor de segurança deve conhecer todas as brechas e fechá-las.
- Os *firewalls* protegem contra acessos explicitamente proibidos, mas e quanto a ataques contra serviços legítimos?
- Quando se adota a 'segurança pela obscuridade', situação em que a organização pensa que sua rede nunca será invadida porque não é conhecida, os responsáveis 'torcem' para que o invasor não saiba dos problemas com segurança e dos valores disponíveis na rede interna. Até quando?
- Novas tecnologias significam novas vulnerabilidades.

- A interação entre diferentes ambientes resulta na multiplicação dos pontos vulneráveis.
- A segurança envolve aspectos de negócios, tecnológicos, humanos, processuais e jurídicos.
- A segurança é complexa.

Estas considerações, segundo Nakamura e Geus (2007, p. 60), mostram "o quanto a segurança é abrangente e multidisciplinar". Cuidar de alguns pontos e negligenciar outros pode comprometer a organização, pois os incidentes sempre ocorrem no elo mais fraco da corrente, ou seja, no ponto mais vulnerável do ambiente.

Independentemente da abordagem escolhida, segundo Beal (2008, p. 25), a avaliação do risco deve ser efetuada por pessoa ou pessoas que detenham:

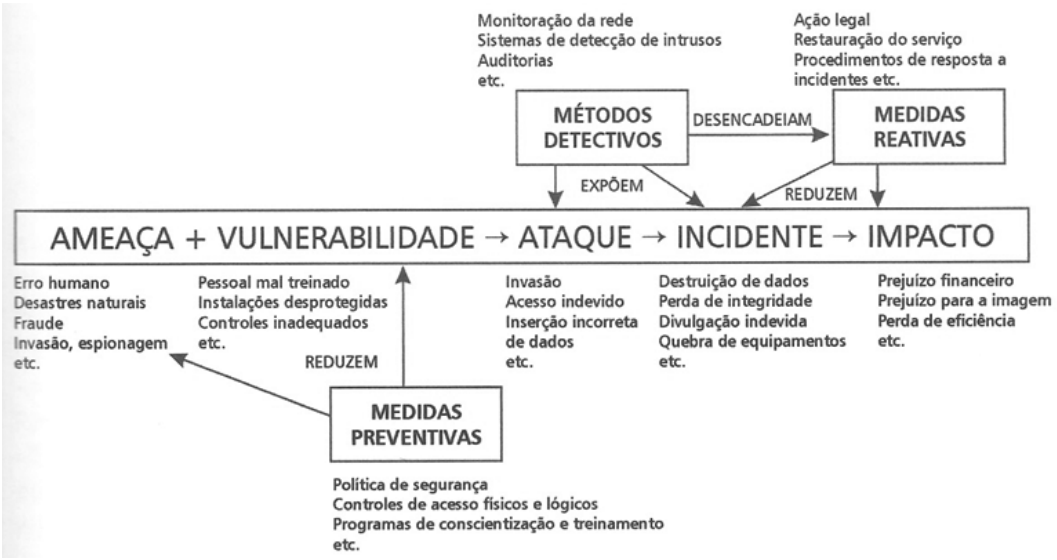
- Entendimento aprofundado do papel e da importância dos ativos de informação sob análise para a organização.
- Formação técnica nas áreas que estão sendo avaliadas.
- Experiência de aplicação dos princípios, procedimentos e práticas de segurança da informação.
- Experiência na metodologia de análise e avaliação de risco a ser empregada, e conhecimento das suas limitações.

3.4 TRATAMENTO DO RISCO

Beal (2008, p. 26) cita que existem várias classificações disponíveis para as medidas de proteção utilizadas para diminuir os riscos de segurança da informação. Uma das classificações possíveis é:

- Medidas preventivas: controles que reduzem a probabilidade de uma ameaça se concretizar ou diminuem o grau de vulnerabilidade do ambiente/ativo/sistema, reduzindo assim a probabilidade de um ataque e/ou sua capacidade de gerar efeitos adversos na organização.
- Medidas corretivas ou reativas: reduzem o impacto de um ataque/incidente. São medidas tomadas durante ou após a ocorrência do evento.
- Métodos detectivos: expõem ataques/incidentes e disparam medidas reativas, tentando evitar a concretização do dano, reduzi-lo ou impedir que se repita.

FIGURA 4 – ETAPAS DA GESTÃO DO RISCO



FONTE: Beal (2008, p. 17)

QUADRO 4 – ETAPAS DA GESTÃO DO RISCO

AMEAÇA	MEDIDAS PREVENTIVAS	MEDIDAS REATIVAS	MÉTODOS DE DETECÇÃO
Fraude.	Supervisão gerencial, segregação de funções, controle efetivo de senhas e permissões de acesso.	Interrupção de pagamentos suspeitos, investigação interna, denúncia à polícia.	Auditoria de *logs*, análise de trilhas de auditoria, conciliação de valores.
Roubo de equipamentos.	Controles de entrada e saída.	Investigação interna, denúncia à polícia.	Inventário periódico, controle de entrada e saída.

FONTE: Adaptado de Beal (2008, p. 17)

Segundo Beal (2008, p. 28),

> os pontos essenciais para tratar adequadamente os riscos elencados pela ISO 17799 são, do ponto de vista legal, proteção de dados e privacidade de informações pessoais, e salvaguarda de registros organizacionais e direitos de propriedade intelectual; e, do ponto de vista das melhores práticas, formalização da política de segurança, educação e treinamento em segurança, relatórios de incidentes e gestão da continuidade do negócio.

Todos esses aspectos de segurança serão analisados ao longo do presente caderno de estudos, e é importante considerar o alerta contido na ISO 17799: nem todos os controles se aplicam ou são viáveis em todas as situações e organizações. A seleção dos controles deve basear-se na análise de risco e de custo/benefício de sua implementação, considerando todos os requisitos de segurança identificados, sejam eles originados das diretrizes internas, legislação vigente ou da própria

avaliação do risco, e os impactos financeiros e não financeiros (para a credibilidade, imagem etc.) associados a estes.

3.5 ACEITAÇÃO DO RISCO RESIDUAL E COMUNICAÇÃO DO RISCO

Selecionadas as medidas de proteção a serem aplicadas, conforme Beal (2008, p. 28), "é preciso comunicar adequadamente o risco residual para a alta direção, para garantir que este seja compreendido e aceito pelos responsáveis globais pela organização, ou, em caso de não aceitação, para permitir que controles adicionais sejam escolhidos para diminuir o nível do risco restante".

Por exemplo, uma solução *single sign-on* (onde um usuário de ambiente computacional informa apenas uma vez sua senha para acessar todos os recursos disponíveis no seu computador e na rede corporativa) pode ser muito conveniente, evitando que, em ambientes mais complexos, o usuário necessite lembrar um grande número de senhas e digitá-las repetidas vezes.

Ao decidir pela aprovação ou não de uma solução desse tipo, a cúpula estratégica precisa considerar o risco adicional associado (uma falha de segurança que leve à divulgação da senha passa a comprometer todo o ambiente computacional, e não apenas alguns recursos, como acontece no caso de senhas separadas). É possível que esse risco possa ser minimizado por medidas adicionais para proteger a senha única, ou que mesmo sem essas medidas o risco seja considerado inferior ao enfrentado quando os usuários precisam manter na memória um número excessivo de senhas (pode-se chegar à conclusão de que, para facilitar o trabalho, eles passam a usar a mesma senha para todos os sistemas, registrá-las em papel ou adotar senhas de fácil adivinhação).

A adequada comunicação dos riscos associados a um e outro caso assegura que a decisão final seja tomada com entendimento claro das implicações de segurança, facilitando a aprovação – se for o caso – de outras despesas consideradas necessárias para implementar controles adicionais que garantam a manutenção dos riscos dentro de níveis considerados aceitáveis pelos dirigentes.

3.6 CONTINUIDADE DOS PROCESSOS DE GESTÃO DO RISCO

De acordo com Beal (2008, p. 29).

> A gestão do risco precisa ser desenvolvida de forma permanente e iterativa, para que mudanças nos sistemas e na forma como são usados, no perfil dos usuários, no ambiente, na tecnologia, nas ameaças, nas vulnerabilidades e em outras variáveis pertinentes não tornem obsoletos os requisitos de segurança estabelecidos. A organização deve programar revisões periódicas da análise de risco, e recalcular as estimativas de risco sempre que seja constatada alguma mudança organizacional com implicações sobre a segurança dos seus ativos de informação.

4 ANÁLISE DO RISCO ECONÔMICO

A finalidade da análise do risco econômico para a segurança, de acordo com Caruso e Steffen (1999, p. 65),

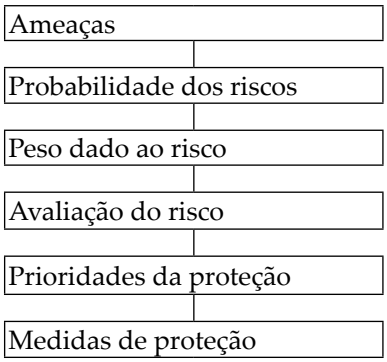
> é obter a medida da segurança existente em determinado ambiente. Essa análise aplica-se também a outras áreas que não a de segurança de informações. Ela envolve aspectos subjetivos em graus variados. A subjetividade irá variar em função do grau de familiaridade que o avaliador tiver em relação ao mecanismo de avaliação, bem como em relação ao ambiente de informações que está sendo avaliado'. Entretanto, sempre restará algum grau de subjetividade no processo, o que não elimina a necessidade da avaliação. Em vez de se contestar a validade da análise, é necessário dar ao avaliador condições para torná-la a melhor possível.

Conforme Caruso e Steffen (1999, p. 66),

> a primeira consideração relacionada com segurança de ativos de informações, como qualquer outra modalidade de segurança, é a relação custo/benefício. Não se despendem recursos em segurança que não tenham retorno à altura, isto é, não se gasta mais dinheiro em proteção do que o valor do ativo a ser protegido. Ainda que existam exceções a essa regra, ela é válida em praticamente todos os casos.

O segundo ponto a ser considerado é que, ainda que o principal fator deva ser a análise da relação custo/benefício, a mesma envolve bom senso. Mesmo nos casos em que não é possível uma análise direta da relação custo/benefício, há meios indiretos de se obterem valores bem próximos dos reais. Um exemplo é o caso de sistemas de computação das companhias aéreas em que toda a operação da companhia é diretamente controlada através de sistemas *on-line*. É difícil justificar a aquisição de um sistema *no-break* somente em função do tempo de processamento perdido; entretanto, o retorno financeiro da aquisição e implantação de uma instalação geradora de energia do tipo *no-break* é mais facilmente justificado em função das receitas oriundas de vendas de passagens, controle da alocação de carga em aeronaves, manutenção programada das aeronaves, controle de estoques de peças, etc. A soma das receitas e dos gastos decorrentes da indisponibilidade pode, facilmente, superar várias vezes o custo de um sistema *no-break*, para cada ocorrência (CARUSO; STEFFEN, 1999).

FIGURA 5 – FLUXO DE ANÁLISE DAS AMEAÇAS E RISCOS



FONTE: Adaptado de Caruso e Steffen (1999, p. 67)

Ainda que frequentemente seja difícil identificar, segundo Caruso e Steffen (1999, p. 67),

> segurança sempre segue parâmetros lógicos, mesmo quando reage a situações de risco criadas por seres humanos; os investimentos relacionados com segurança podem facilmente chegar à casa de milhões de dólares com o consequente custo indireto relacionado. A forma mais eficiente de se efetuar a análise de custo/benefício é fazer com que os usuários finais de cada sistema de informações avaliem o valor das mesmas para a organização; quem trabalha com as informações no seu dia a dia é o mais indicado para fazer a análise de risco.

Uma metodologia relativamente simples para auxiliar na decisão dos investimentos de segurança, principalmente quando é difícil avaliar valores monetários, mas há um elevado risco para a imagem ou qualquer fator subjetivo, segundo Caruso e Steffen (1999, p. 68), consiste nas etapas:

- Análise dos riscos e suas consequências.
- Estimativa das probabilidades de ocorrência.
- Estimativa do dano causado pela ocorrência do incidente (vulnerabilidade).
- Cálculo da exposição: E = V x P, onde V é a vulnerabilidade ou dano financeiro causado pela ocorrência do incidente e P é a probabilidade da ocorrência em vezes/ano.
- Análise das medidas de proteção contra os riscos.
- Seleção das medidas de proteção a implementar, em função da relação custo/eficácia da segurança.

> Um exemplo prático resultante dessa análise está relacionado com as instalações do tipo *no-breaks* e geradores. É frequente a queda de energia em muitas cidades e até mesmo em áreas extensas do país; em alguns locais ocorre várias vezes por dia. Por isso, devido à incidência e aos transtornos de perda de tempo e retomadas é fácil concluir que esse investimento é indispensável em muitos dos casos, a exemplo das empresas aéreas. (CARUSO; STEFFEN, 1999, p. 68).

Segundo Caruso e Steffen (1999, p. 68), "casos de incêndio não são frequentes, mas caso ocorram, sua consequência é um desastre completo e de difícil recuperação".

FIGURA 6 – PROBABILIDADE DOS RISCOS E SUAS CONSEQUÊNCIAS

Risco = Probabilidade X grau das consequências

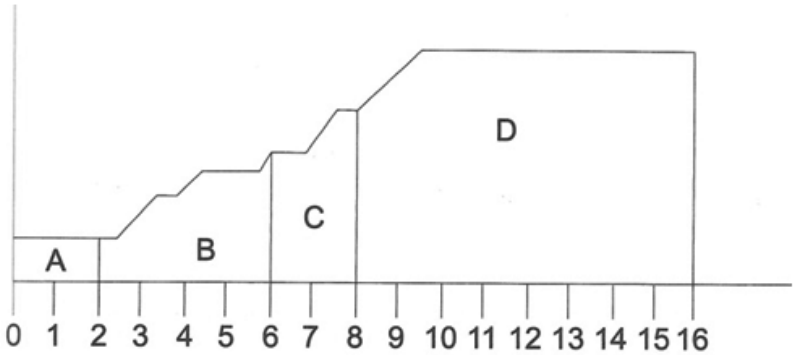
Riscos	
Peso	Probabilidade
1	Extremamente improvável
2	Improvável
3	Possível
4	Bem possível/já aconteceu

Consequências	
Peso	Grau
1	Insignificante
2	Médio
3	Grande
4	Põe em perigo a existência da empresa

FONTE: Adaptado de Caruso e Steffen (1999, p. 68)

Aplicando-se a fórmula acima na avaliação dos riscos e suas consequências, obtêm-se as prioridades de proteção, conforme demonstrado no gráfico a seguir:

FIGURA 7 – PRIORIDADES DE PROTEÇÃO



Prioridades da proteção
A – pouca ou nenhuma
B – baixa
C – média
D – alta

FONTE: Caruso e Steffen (1999, p. 69)

A partir daí, conforme Caruso e Steffen (1999, p. 69), "devem-se relacionar as medidas de proteção para cada caso".

Como em qualquer outra atividade empresarial, o capital investido em informática corre os mesmos riscos de destruição, roubo, violação, fraude etc. que o capital empregado em outro tipo de atividade, digamos, um supermercado ou um banco. "Esses ativos são representados por instalações, equipamentos, *softwares* e dados. Dos quatro, os dois últimos são de longe os mais valiosos, sendo que o último pode vir a ser insubstituível". (CARUSO; STEFFEN, 1999, p. 69).

Inerente aos sistemas de informações, de acordo com Caruso e Steffen (1999, p. 70),

> temos o fato de que as próprias informações dos aplicativos representam, por si sós, os fatores de produção empregados nos negócios que estas operações representam. Portanto, uma boa fonte de análise é a própria operação de negócio; o negócio em si é, normalmente, muito bem documentado e os executivos das diversas áreas conhecem muito bem o valor das operações que gerenciam para a organização.

Como em qualquer outra atividade humana, segundo Caruso e Steffen (1999, p. 70), o processamento de informações e as atividades ligadas às informações ainda não podem prescindir do uso de mão de obra com graus variados de especialização. Na realidade, a mão de obra é o componente de custo com a participação percentual mais elevada dentro de um ambiente de informações, principalmente em decorrência da constante queda de preços do *hardware*, em termos de unidade de informação processada pelo valor investido em equipamentos. Esse custo de mão de obra passa a integrar o custo dos ativos nos quais ela foi empregada (sistemas operacionais, sistemas de aplicações etc.), que irão constituir as ferramentas de processos dentro do ambiente de informações.

Ainda segundo Caruso e Steffen (1999, p. 70),

> em ambientes de informações e informática, temos duas classes principais de materiais em processo, a saber: o acervo de informações destinadas a confeccionar as ferramentas de processamento de informações ou sistemas de programas de aplicações ou de controle da atividade e informações relacionadas com as atividades dentro das empresas, que serão processadas pelos sistemas informatizados.

Além disso, temos que ter sempre em conta que não existe informação sem custo; mesmo em casos em que as informações são obtidas sem nenhum custo, a estrutura organizacional e de recursos necessária para a coleta tem um custo, que é rateado em cima de cada unidade de informação coletada.

Ainda que as informações possam não receber um tratamento físico-contábil igual ao dado a outros ativos, conforme Caruso e Steffen (1999, p. 70), elas devem ser consideradas como ativos dentro das empresas, quando não para poderem ser objetos de avaliação quanto a medidas de segurança a serem adotadas visando à sua proteção.

Não existe nenhuma metodologia 100% eficaz para se fazer análises de custo/benefício. Praticamente todas as metodologias existentes atualmente contemplam somente parte do problema da análise de custo/benefício ou estão direcionadas aos aspectos de descarte das informações.

A maior crítica recebida pelas metodologias de análise de risco em geral consiste no grau de subjetividade que o ativo avaliado apresenta para o proprietário do mesmo. Entretanto, estas críticas não invalidam a necessidade de se efetuar tal análise, visto que o problema não reside na metodologia em si, mas está relacionado com o grau de conhecimento que o avaliador possui quanto ao ativo avaliado. Além disso, mesmo que subjetivas, as metodologias fornecem parâmetros relativamente seguros para se avaliar o grau de importância de cada ativo para a organização. É preferível uma avaliação com algum grau de subjetividade a desconhecer totalmente

a extensão dos riscos que podem afetar os ativos da organização (CARUSO; STEFFEN, 1999).

O fundamental para que a metodologia funcione de forma adequada, de acordo com Caruso e Steffen (1999, p. 71),

> é uma avaliação correta da importância dos ativos e dos riscos a que eles estão sujeitos. Devido a isso, é importante que a avaliação seja conduzida pelo responsável pelo ativo avaliado, assessorado por um especialista em segurança (nas organizações em que ele existir, uma boa fonte de assessoria quanto a riscos em geral pode ser a área atuarial, que é responsável pelos seguros).

Somente o responsável pelo ativo conhece a sua importância real para a organização e o nível de risco a que o mesmo pode estar sujeito; a possível subjetividade do processo não altera o fato de que existem riscos e que os mesmos devem ser avaliados.

Conforme Caruso e Steffen (1999, p. 71), "a primeira coisa a ser feita no âmbito da análise de risco econômico da segurança é determinar quais fatores afetam a segurança dos ativos que serão avaliados". São dois os principais fatores envolvidos:

- Grau de impacto da ocorrência.
- Nível de exposição à ocorrência.

O primeiro item deve tratar das consequências que uma ocorrência danosa provocaria para a organização e o segundo deve listar os riscos a que cada ativo está sujeito.

Dentro de uma organização, suas diversas áreas sofrem de forma desigual as consequências de uma ocorrência danosa ao seu funcionamento, quer essa ocorrência afete ativos, quer afete processos; dentro da mesma área, as consequências variam em função dos ativos ou processos afetados. Ainda que cada organização seja em certa medida única, segundo Caruso e Steffen (1999, p. 72), a grosso modo podemos classificar os impactos conforme o quadro a seguir.

QUADRO 5 – ETAPAS DA GESTÃO DO RISCO

Alto risco	A organização como um todo, ou parte importante da mesma, tem suas atividades fortemente reduzidas a curto ou médio prazo, não permitindo a continuidade normal de suas atividades, ou até mesmo pondo em risco a sobrevivência da organização.
Médio risco	As atividades da organização, ou de parte da mesma, sofrem dificuldades sérias, que acarretam prejuízos sensíveis, mas que não chegam a afetar a sobrevivência da organização como um todo.
Baixo risco	As atividades da organização não são afetadas de forma significativa pela ocorrência.

FONTE: Adaptado de Caruso e Steffen (1999, p. 72)

Cada atividade, processo ou produto dentro de uma organização está exposto a certo grau de risco que lhe é inerente; os riscos existem associados a quaisquer atividades. "O nível de exposição está diretamente relacionado com a probabilidade de ocorrência de um evento danoso para um determinado ativo". (CARUSO; STEFFEN, 1999, p. 72).

Frequentemente, a própria atividade da organização é, conforme Caruso e Steffen (1999, p. 72),

> um fator de risco para sua sobrevivência, a exemplo de uma refinaria de petróleo, em que os riscos de incêndio são muito grandes. A interligação de seu ambiente de informações com a internet aumenta exponencialmente os riscos a que suas informações e seus equipamentos estão sujeitos.

Para isto, de acordo com Caruso e Steffen (1999, p. 72), "é importante fazer uma avaliação mais precisa possível do nível de exposição, caso o mesmo não possa ser reduzido ou a própria exposição eliminada, e estar preparado para suas eventuais ocorrências, de modo que sejam ao máximo evitadas; mas, no caso de as mesmas virem a acontecer, é importante ter medidas de segurança prontas para serem ativadas".

5 CLASSIFICAÇÃO DE INFORMAÇÕES

Segundo Ferreira e Araújo (2008, p. 78), "a classificação de informações é o processo no qual se estabelece o grau de importância das informações conforme seu impacto no negócio. Quanto mais decisiva e estratégica para o sucesso ou manutenção da organização, maior será sua importância".

"A classificação deve ser realizada a todo instante, em qualquer meio de armazenamento". (FERREIRA; ARAÚJO, 2008, p. 78).

Existem regras que devem ser consideradas durante a classificação e, segundo Ferreira e Araújo (2008, p. 78), "a principal delas é a determinação de proprietários para todas as informações, sendo este o responsável por auxiliar na escolha do meio de proteção".

Ainda conforme Ferreira e Araújo (2008, p. 78),

> nos casos onde houver um conjunto de informações armazenadas em um mesmo local, e elas possuírem diferentes níveis, deve-se adotar o

critério de classificar todo o local com o mais alto nível de classificação. As informações armazenadas em qualquer local devem estar de acordo com os critérios de classificação e devem possuir uma identificação que facilite o reconhecimento do seu grau de sigilo.

"Toda informação classificada, quando passar por alteração de conteúdo, deve ser submetida a novo processo de classificação, com o objetivo de rever o nível mais adequado". (FERREIRA; ARAÚJO, 2008, p. 79).

Para iniciar o processo de classificação "é necessário conhecer o negócio da organização, compreender os processos e atividades realizadas e, a partir deste momento, iniciar as respectivas classificações". (FERREIRA; ARAÚJO, 2008, p. 79).

Conforme o quadro a seguir, as organizações podem utilizar um inventário dos ativos de informações:

QUADRO 6 – INVENTÁRIO DOS ATIVOS DE INFORMAÇÕES

NATUREZA DO ATIVO	**ATIVOS DE INFORMAÇÃO**
Informação	Banco de dados e arquivos magnéticos. Documentação de sistemas e manual do usuário. Material de treinamento. Procedimentos operacionais de recuperação. Planos de continuidade.
Documento em papel	Contratos. Documentação da empresa. Relatórios confidenciais.
Software	Aplicativos. Sistemas operacionais. Ferramentas de desenvolvimento. Utilitários do sistema.
Físico	Servidores, *desktops* e *notebooks*. Impressoras e copiadoras. Equipamentos de comunicação (*fax*, roteadores). Mídias magnéticas. Gerador, *no-break* e ar-condicionado. Móveis, prédios e salas.
Pessoa	Empregados, estagiários, terceiros e fornecedores.
Serviço ou atividade	Computação (aplicação de *patches*, *backup*). Comunicação (ligações telefônicas, videoconferências). Utilidades gerais.

FONTE: Adaptado de Ferreira e Araújo (2008, p. 78-79)

É de suma importância, de acordo com Ferreira e Araújo (2008, p. 79), estabelecer algumas definições no início do processo:

- **Classificação**: é a atividade pela qual se atribuirá o grau de sigilo às informações, sejam meios magnéticos, impressos etc.
- **Proprietário**: é o profissional de uma determinada área responsável pelos ativos de informação da organização.
- **Custodiante**: trata-se do profissional responsável por assegurar que as informações estejam de acordo com o estabelecido pelo proprietário da informação.
- **Criptografia**: é uma codificação que permite proteger documentos contra acessos e/ou alterações indevidas.
- **Perfil de acesso**: trata-se de uma definição de direitos de acesso às informações, transações, em meios magnéticos ou impressos de acordo com a necessidade de uso de cada usuário.

5.1 NÍVEIS DE CLASSIFICAÇÃO

Uma vez que os critérios de classificação estejam adequadamente definidos e implementados, segundo Ferreira e Araújo (2008, p. 80), "deve-se determinar a classificação que será utilizada e os controles de segurança adequados". Fatores especiais, incluindo exigências legais, devem ser considerados no momento de estabelecer a classificação.

> Muitas classificações não são aconselhadas, pois poderão gerar confusões para os proprietários das informações e/ou encontrar algum tipo de resistência para sua implementação. A equipe não deve permitir que as áreas do negócio utilizem classificações diferentes daquelas especificadas nas políticas da organização. (FERREIRA; ARAÚJO, 2008, p. 80).

Conforme Ferreira e Araújo (2008, p. 80), cada classificação deve ser de fácil compreensão e claramente descrita para demonstrar a diferenciação entre cada uma delas, devendo-se evitar níveis excessivos de classificação. Segundo os autores, três níveis podem ser suficientes para uma boa prática de classificação da informação, a saber:

I. Classe 1 – Informação pública: Informações que não necessitam de sigilo algum, podendo ter livre acesso para os colaboradores. Não há necessidade de investimentos em recursos de proteção. São informações que, caso sejam divulgadas fora da organização, não trarão impactos para os negócios. Exemplos: testes de sistemas ou serviços sem dados confidenciais; brochuras / *folders* da organização; as demonstrações financeiras de uma organização após serem publicadas em um jornal tornam-se públicas, no entanto, enquanto estão na contabilidade da organização são confidenciais.

II. Classe 2 – Informação interna: O acesso externo às informações deve ser evitado. Entretanto, se esses dados tornarem-se públicos, as consequências não serão críticas. A integridade dos dados é vital. Exemplos: agendas de telefones e

ramais; os benefícios que a organização oferece aos seus empregados podem ser classificados para uso interno, pois não faz sentido divulgar essas informações para outras organizações, no entanto, é de livre acesso para todos os seus empregados.

III. Classe 3 – Informação confidencial: As informações desta classe devem ser confidenciais dentro da organização e protegidas do acesso externo. Se alguns desses dados forem acessados por pessoas não autorizadas, as operações da organização poderão ser comprometidas, causando perdas financeiras e de competitividade. A integridade dos dados é vital. Exemplos: salários, dados pessoais, dados de clientes, estratégias de mercado e senhas.

5.2 ARMAZENAMENTO E DESCARTE DE INFORMAÇÕES CLASSIFICADAS

De acordo com Ferreira e Araújo (2008, p. 81), "qualquer informação deve ser tratada de acordo com seu impacto no negócio. Os recursos e investimentos realizados para a proteção devem estar condicionados a esse fator". Os processos de armazenamento e descarte de uma informação devem ser desenvolvidos para atender às necessidades de confidencialidade da informação.

QUADRO 7 – CRITÉRIOS DE ARMAZENAMENTO E DESCARTE DE INFORMAÇÕES

Informações públicas	Armazenamento: devem ser armazenadas com a utilização de recursos considerando o menor investimento, sem a preocupação com confidencialidade.
	Descarte: pode-se proceder de forma simples, sem o uso de recursos e procedimentos.
Informações internas	Armazenamento: as informações com tal classificação devem ser armazenadas de acordo com a necessidade, em áreas de acesso reservado.
	Descarte: tais informações devem ser descartadas utilizando-se recursos e procedimentos específicos. As informações confidenciais devem servir de base para o desenvolvimento do processo e aquisição dos recursos.
Informações confidenciais	Armazenamento: os locais onde as informações estão armazenadas devem possuir acessos controlados, havendo uma concessão formal e por meio de procedimento que envolva o proprietário da informação.
	Descarte: deve ser efetuado por meio de procedimentos e ferramentas que destruam a informação por completo.

FONTE: Adaptado de Ferreira e Araújo (2008, p. 82)

5.3 PUBLICAÇÃO DE INFORMAÇÕES NA WEB

De acordo com Ferreira e Araújo (2008, p. 82), "as informações somente devem ser divulgadas externamente quando devidamente autorizadas. A divulgação na internet ou extranet é destinada somente para as informações públicas".

5.4 PERDA OU ROUBO DE INFORMAÇÕES

Conforme Ferreira e Araújo (2008, p. 83), "na ocorrência de perda efetiva ou suspeita da quebra da confidencialidade da informação, por quaisquer motivos, deve-se comunicar formalmente a área responsável sobre o ocorrido".

> As investigações devem ser realizadas por meio de práticas previamente estabelecidas e obrigatoriamente já divulgadas por todos os profissionais através de uma política formalmente aceita e pela assinatura do termo de confidencialidade. (FERREIRA; ARAÚJO, 2008, p. 83).

5.5 MONITORAMENTO CONSTANTE

Após a classificação das informações, deve-se elaborar e implementar procedimentos para o monitoramento contínuo, segundo Ferreira e Araújo (2008, p. 83). A área de Segurança da Informação, junto com os proprietários da informação, deve periodicamente revisar as informações classificadas para assegurar que elas estejam adequadamente classificadas.

Adicionalmente, de acordo com Ferreira e Araújo (2008, p. 83), os privilégios e direitos de acesso dos usuários também devem ser revisados para assegurar que estejam de acordo com as necessidades de cada usuário.

6 DIREITOS DE ACESSO

Associado ao acúmulo de funções e seu consequente acesso às informações relacionadas com essas funções, de acordo com Caruso e Steffen (1999, p. 91), "aparece o direito de determinado indivíduo de acessá-la. No passado, o direito de acesso a informações baseava-se em regras militares (autoritárias) ou em regras acadêmicas (amigáveis). Um sistema de aplicações comerciais não pode ser tão restrito quanto às aplicações militares, nem tão aberto quanto às aplicações acadêmicas". Em nenhum dos casos acima há preocupação com a fonte da autoridade para conceder direitos de acesso, pois no caso de aplicações militares o acesso é controlado por regulamentos rígidos e no caso de aplicações acadêmicas não se discute a questão do direito de acesso.

Para cada caso, segundo Caruso e Steffen (1999, p. 91), a fonte da autoridade deve estar claramente definida na política de segurança da organização. As regras de controle de acesso devem levar em conta os cinco componentes da política de controle de acesso:

- Usuários: pessoas ou funções associadas a pessoas que acessam recursos em um ambiente de informações.
- Recursos: constituem o conjunto de equipamentos, informações ou ferramentas de apoio ou de execução final das tarefas que os usuários precisam executar.

- Operações: o nível de acesso permitido a cada usuário em relação aos recursos colocados à sua disposição. Cada recurso é passível de certo número de operações e estas somente podem ser executadas por determinados usuários.
- Autoridade: quem detém o poder de decisões; essa autoridade pode ser primária, decorrente da posse, ou secundária ou delegada, decorrente da transferência parcial ou total de autoridade oriunda de nível mais elevado. O conceito de autoridade está ligado ao conceito de propriedade; em princípio quem tem a posse de determinado recurso pode delegar autoridade, determinar direitos de guarda ou custódia ou determinar quem administra o direito de acesso em seu lugar.
- Domínio: os limites dentro dos quais se aplica a autoridade; um domínio pode conter recursos, usuários ou recursos e usuários. O domínio determina os limites dentro dos quais se aplica a autoridade do proprietário ou do delegado que a exerce em seu nome.

6.1 AUTORIDADE

Em organizações comerciais e industriais, de acordo com Caruso e Steffen (1999, p. 92),

> a autoridade é o poder legítimo para controlar ou administrar. Existem dois tipos de autoridade: a relacionada com pessoas e a relacionada com recursos. Um administrador (de segurança, no caso de ambientes de informações) precisa ter autoridade tanto sobre pessoas como sobre recursos, para poder conceder direitos de acesso.

Além disso, é possível que as regras determinem que ele mesmo não possa ter direito de acessar os recursos para os quais concede direito de acesso. Portanto, deve-se separar o direito de acesso do direito de conceder acesso; "o primeiro é decorrente da necessidade legítima de executar funções que façam uso de recursos protegidos, ao passo que o segundo é decorrente da delegação de autoridade por parte do legítimo proprietário, e essa delegação de autoridade não precisa necessariamente abranger o próprio direito de o administrador acessar o recurso que vai administrar em nome do proprietário". (CARUSO; STEFFEN, 1999, p. 92).

Ainda conforme Caruso e Steffen (1999, p. 92), a autoridade envolve dois domínios: o domínio organizacional, ou sobre usuários, e o domínio sobre recursos. Na figura X é mostrado um modelo simplificado de um ambiente de informações, com um domínio de recursos e um domínio organizacional e as interações entre ambos:

- Domínio organizacional: é o que define os limites dos usuários ou grupos de usuários dentro de uma organização. Normalmente são definidos com base nas posições ocupadas pelos usuários dentro da organização; é para esses domínios organizacionais que os administradores de segurança exercem seus serviços. A área de atuação dos administradores de segurança pode abranger toda a organização ou partes dela. Um administrador de segurança só pode conceder direito de acesso a indivíduos que façam parte do domínio organizacional para o qual foi autorizado.

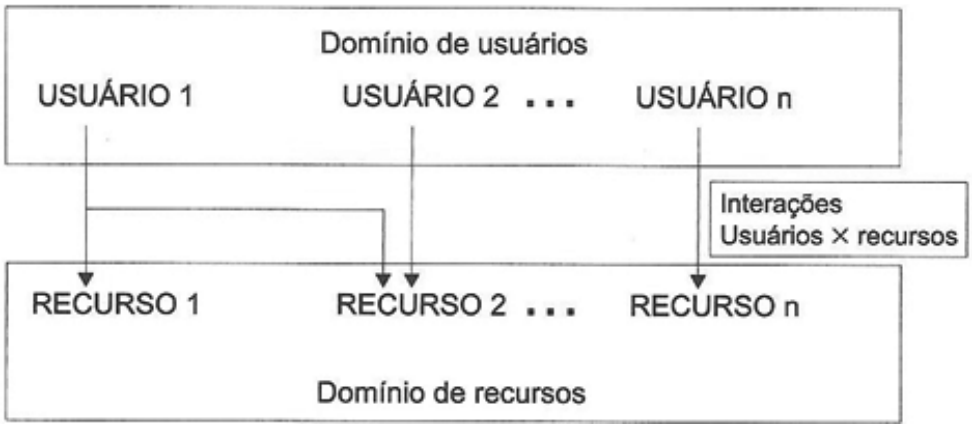
- Domínio de recursos: é o conjunto de operações – executadas por meio de recursos aos quais o administrador de segurança tenha o direito de conceder acesso – que o mesmo pode autorizar que usuários ou grupos de usuários de determinado domínio executem em função de necessidade de suas tarefas. Um administrador de segurança só pode conceder direito de acesso a recursos que façam parte do domínio de recursos que administra.

> O sistema de segurança deve permitir que administradores de segurança concedam acesso somente se o recurso e o receptor do direito de acesso estiverem dentro do domínio organizacional e do domínio de recursos sobre os quais determinado administrador de segurança tenha autoridade. Qualquer acesso cruzado, envolvendo domínios de administradores de segurança diferentes, deve, necessariamente, passar pelo crivo do proprietário do domínio dos recursos a serem acessados, ou então deve estar previsto que os administradores de segurança tenham autoridade para tanto. (CARUSO; STEFFEN, 1999, p. 93).

De qualquer forma, segundo Caruso e Steffen (1999, p. 93),

> não pode ser dado direito de acesso diretamente por um administrador de determinado domínio organizacional em cima de domínio de recursos sobre o qual não tenha autoridade; nem um administrador de determinado domínio de recursos pode dar diretamente direito de acesso para usuário de domínio organizacional que não o seu.

FIGURA 8 – MODELO SIMPLIFICADO DE DOMÍNIOS EM UM AMBIENTE DE INFORMAÇÕES



FONTE: Caruso e Steffen (1999, p. 93)

6.2 A FONTE DA AUTORIDADE

Conforme Caruso e Steffen (1999, p. 93), "a fonte da autoridade sobre ativos emana de seus proprietários. O conceito de proprietário, para fins de controle de acesso, está diretamente relacionado com o conceito de necessidade de uso em decorrência da função exercida".

"No sentido mais restrito, os proprietários dos ativos de uma organização são seus acionistas; entretanto, na maioria das grandes organizações a propriedade de ativos está separada de sua administração, de modo que os proprietários delegam a autoridade para administrar em seu nome". (CARUSO; STEFFEN, 1999, p. 94).

Com base no exposto acima, ainda segundo Caruso e Steffen (1999, p. 94),

> em um ambiente de informações o proprietário de um recurso é quem exerce controle sobre ele. Esse conceito de propriedade parece-se mais com o conceito de custódia, em que a pessoa que controla o recurso não tem sua posse real, mas exerce o controle sobre o mesmo como se fosse o proprietário real e responde por sua integridade perante o proprietário real.

Esse conceito, de acordo com Caruso e Steffen (1999), é semelhante ao aplicado na elaboração de um orçamento financeiro, em que o mesmo é aprovado pela administração da organização e dividido entre suas principais funções organizacionais. Cada uma dessas funções principais da empresa torna a dividir os recursos financeiros que lhe cabem entre as subfunções que lhe são subordinadas. Cada uma dessas "divisões" orçamentárias conhece a extensão do seu orçamento, os limites de sua autoridade e as responsabilidades envolvidas, e presta contas em função desse fato.

No início da era da informática, em função da complexidade das tarefas envolvendo o desenvolvimento de aplicações, conforme Caruso e Steffen (1999, p. 94), "surgiu o conceito de que os ativos informatizados da empresa eram de propriedade da área de informática. Assim que determinada área contratava a execução de serviços seus em computadores, ela transferia os direitos de propriedade sobre os ativos envolvidos para a área de informática".

Esse conceito, além de não ser natural, implicava um poder muito grande nas mãos dos administradores da área de informática. Atualmente, em decorrência da evolução da própria informática, com custos cada vez mais reduzidos e ferramentas cada vez mais poderosas, e em decorrência da evolução de muitas funções para suas áreas de origem, inclusive com pessoal de desenvolvimento alocado nas áreas afins, o conceito de propriedade tem-se firmado como sendo da pessoa responsável pelos ativos de informações processados pelos computadores e não mais dos responsáveis pela área de informática. O direito de propriedade sobre ativos deve ser separado da responsabilidade pela manutenção da integridade dos ativos, que nem sempre compete ao seu proprietário (CARUSO; STEFFEN, 1999).

Caruso e Steffen (1999, p. 94) afirmam que o direito de acesso deve ser definido formalmente, como qualquer outra responsabilidade dentro de uma organização, e deve incluir os critérios para sua delegação. A cadeia de delegação da autoridade deve ser passível de controle em ambos os sentidos e deve estar baseada na fonte da autoridade, a partir do conselho diretor da empresa. Podem ser delegadas três classes de direitos:

- Propriedade – permite o controle total de um recurso.
- Delegar direitos – permite que o possuidor desse tipo de autoridade delegue a terceiros o direito de acesso.
- Direito de acesso – permite que o receptor execute operações específicas com o recurso.

O direito de acesso está ligado diretamente ao nível do direito concedido e, de acordo com Caruso e Steffen (1999, p. 95), deve obedecer à regra do "menor privilégio possível". Geralmente, o direito de acesso em um nível mais amplo inclui o direito de acesso em um nível mais restrito. As principais ferramentas de controle de acesso a ambientes de informações baseiam-se na estrutura de delegação de autoridade, separando o papel do administrador de segurança do acesso normal e da propriedade sobre os recursos que o administrador controla.

6.3 REQUISITOS QUE REGULAM O DIREITO DE ACESSO EM EMPRESAS

Nas empresas, conforme Caruso e Steffen (1999, p. 95), "são três os principais requisitos que governam o direito de acesso: proteção de ativos, práticas de auditoria e legislação".

6.3.1 Proteção de ativos

Segundo Caruso e Steffen (1999, p. 94), "o acervo informacional de uma empresa também se constitui em ativo e, como tal, precisa ser protegido. Os ativos a serem protegidos caracterizam os domínios de recursos; esses domínios de recursos incluem o acervo de informações, as ferramentas de apoio e de acesso ao domínio e sua mídia de suporte".

A proteção de ativos torna-se cada vez mais necessária em função da concentração de informações em computadores; ela implica a proteção dos recursos de informações contra ameaças resultantes de danos ou deturpação de recursos do domínio. As ameaças mais frequentes aos recursos de um domínio são: danos físicos em equipamentos usados para suportar o acervo de informações, que podem ser resultantes de ações acidentais ou deliberadas de usuários ou terceiros, ou, então, causadas por acidentes naturais; revelação não autorizada, acidental ou deliberada, de informações de natureza confidencial e fraudes.

De acordo com Caruso e Steffen (1999, p. 95),

> a fraude em si é o tipo de ameaça que mais tem atraído as atenções. O potencial de manipulação que os sistemas informatizados permitem, inclusive a distância, é muito grande, ainda que os casos apurados sejam poucos em relação ao total. E esse risco aumenta exponencialmente à medida que as organizações abrem seus sistemas informacionais para terceiros através de redes públicas de acesso, como a Internet.

6.3.2 Práticas de auditoria

"As práticas de auditoria surgiram a partir do crescente distanciamento dos proprietários dos ativos em relação ao seu controle direto em cima dos mesmos; a auditoria visa proteger os proprietários quanto ao seu direito de propriedade sobre ativos em relação aos quais eles não têm mais controle direto". (CARUSO; STEFFEN, 1999, p. 96).

Caruso e Steffen (1999, p. 96) citam que,

> a função da auditoria em ambientes de informações é garantir que os sistemas de informações funcionem de forma adequada, permitindo que as funções necessárias sejam executadas ao mesmo tempo que a integridade dos ativos seja garantida. Isso inclui o controle sobre os domínios de recursos e de usuários, a forma como os usuários de determinado domínio de usuários acessam diferentes domínios de recursos e as operações permitidas para cada usuário em cada domínio de recursos.

6.3.3 Legislação

Conforme Caruso e Steffen (1999, p. 96),

> em alguns países existem leis que regulam claramente as responsabilidades de usuários e de administradores de recursos de informações em geral; em outros ainda não existem dispositivos legais claros a respeito do assunto, ou quando existem não são claros ou completos. Onde existem, a legislação determina as responsabilidades gerais de administradores em relação à proteção aos ativos e as penalidades previstas.

Entretanto, ainda conforme Caruso e Steffen (1999, p. 96), "mesmo em países que ainda não tenham legislação acerca do assunto, os administradores de empresas multinacionais devem estar atentos para a legislação específica (onde for o caso) dos países-sede dessas empresas". Por exemplo, a legislação americana responsabiliza os administradores de suas filiais no exterior em relação à segurança de informações; ainda que essa lei não possa ser aplicada a cidadãos de outros países que trabalhem para empresas americanas fora dos Estados Unidos, ela os afeta na medida em que a matriz impõe uma política de segurança fundamentada nessa lei, obrigando seus funcionários a cumprirem de forma indireta, dentro das normas internas da empresa, como forma de ascensão profissional dentro da organização.

6.4 CONTROLES SOBRE O DIREITO DE ACESSO

Segundo Caruso e Steffen (1999, p. 96), "são métodos empregados para controlar o acesso que cada usuário de determinado domínio tem sobre recursos de determinado domínio de recursos". Esses métodos de controle devem ser de dois tipos: controles organizacionais e controles operacionais.

6.4.1 Controles organizacionais

São regulamentos internos que contemplam as diversas atividades da organização; não são específicos para informações nem devem basear seus princípios exclusivamente em legislação que cuide do assunto. Os controles operacionais em informática também devem basear-se neles, devendo inspirar-se nos mesmos princípios que qualquer outra atividade de usuários dentro de uma organização, principalmente na autorização da operação e no princípio da segregação de funções. Nenhuma operação deve ser tão abrangente que implique o controle total ou muito grande envolvendo ativos; isso é decorrente do princípio da segregação de funções e é decisivo para melhor controlar o potencial para fraudes, existente em qualquer atividade exercida por seres humanos (CARUSO; STEFFEN, 1999).

6.4.2 Controles operacionais

Ainda que relacionados em um item separado em relação aos controles organizacionais, de acordo com Caruso e Steffen (1999, p. 97), "na prática não passam da aplicação dos controles organizacionais ao ambiente de informações". No passado, esses controles eram baseados em senhas de acesso associadas a recursos individuais dentro de grupos, a grupos de recursos dentro de domínios ou a todo um domínio de recursos; entretanto, esse método é fraco em virtude de problemas relacionados com o compartilhamento de recursos e com a necessidade de identificação e responsabilização individual de usuários, o que não é possível com esse método. Atualmente usam-se cada vez mais métodos associados com a identificação de usuários, listas de acesso e privilégios de uso, permanecendo o mecanismo de senhas somente com método de autenticação da identidade de usuários.

> As listas de acesso devem definir claramente que operações cada usuário pode executar dentro de um domínio de recursos e a forma como essas operações devem ser executadas. Esse princípio deve ficar claro, pois é com base nele que as ferramentas de segurança trabalham ao permitir ou negar acesso de usuários a determinados recursos. (CARUSO; STEFFEN, 1999, p. 97).

6.5 QUEM CONTROLA O "CONTROLADOR"?

Conforme Caruso e Steffen (1999, p. 97), "essa pergunta não apareceu com os sistemas informatizados; ela remonta à antiguidade". Sua idade indica que ainda não existe uma resposta completa e final. A questão real é saber exatamente como controlar alguém que detém o direito de conceder direito de acesso a outras pessoas sem que essa mesma pessoa acesse os recursos que controla, uma vez que ela tem poder para obter esse acesso, ainda que ilegítimo. Em princípio a resposta é: *Nada pode impedir tal tipo de ato*. Entretanto, os riscos podem ser minimizados pelas seguintes medidas:

- Limitar o tamanho do risco – por meio de limites à autoridade do administrador, por exemplo, restringindo o domínio de recursos sobre o qual um administrador de segurança exerce controle.
- Reduzir a probabilidade de ocorrência – pela segregação de funções, definindo o domínio organizacional sobre o qual um administrador de segurança exerce controle e dando o controle sobre o administrador de segurança para outra pessoa.
- Tornar os riscos detectáveis – pelo controle sobre as atividades dos administradores de segurança exercido por pessoas de fora da estrutura de segurança. Esse controle deve, em princípio, ser exercido pelo pessoal de auditoria. Os atos dos administradores de segurança devem ser mantidos sob estrito controle. (CARUSO; STEFFEN (1999, p. 97).

6.6 CONSIDERAÇÕES GERAIS SOBRE DIREITO DE ACESSO

De acordo com Caruso e Steffen (1999, p. 98), uma política de controle de acesso a recursos deve considerar algumas regras básicas, de modo que as decisões baseadas na política de controle de acesso sejam coerentes e consistentes com as diretrizes da política geral de segurança da empresa. Essas regras de política devem incluir:

- Controle de acesso feito em função da posição ocupada por pessoas e não em função de pessoas que eventualmente as ocupem.
- Controle exercido por administrador de segurança sobre pessoas, restrito somente ao seu domínio organizacional.
- Controle exercido por administrador de segurança sobre recursos, restrito somente ao seu domínio de recursos.
- Domínios organizacionais definidos por administradores que exerçam controle sobre os mesmos, podendo a autoridade, para dar direitos de acesso a esses domínios, ser delegada a um administrador de segurança.

- Domínios de recursos definidos por administradores que exerçam controle sobre os mesmos, podendo a autoridade, para dar direitos de acesso a esses domínios, ser delegada a um administrador de segurança.
- Se uma pessoa que ocupa determinada posição dentro de um domínio organizacional tiver acesso a determinado domínio de recursos, ela deve ser capaz de acessar todos os subdomínios contidos dentro do mesmo, a menos que exista regra mais específica que controle o acesso a subdomínios desse domínio.
- O administrador de segurança que concede o direito de acesso a um domínio de recursos deve aplicar os controles sobre os acessos feitos pelo receptor desse direito.
- O administrador de segurança deve ter o efetivo controle sobre o direito de dar acesso sobre o domínio de recursos que administra.
- Em domínios organizacionais estruturados de forma hierárquica, os usuários devem ser colocados em estruturas organizacionais que reflitam a estrutura organizacional da empresa.
- A propriedade ou a custódia de recursos deve refletir a delegação de autoridade derivada da estrutura de autoridade.
- Onde for o caso, deve definir os critérios de outorga de direitos de acesso de um usuário para outro; por exemplo, um usuário pode outorgar a outro o direito de acesso a informações que tenha criado, mas somente nesse caso.

Uma lista de diretrizes de direito de acesso poderia incluir centenas de itens; entretanto, isso poderia tornar-se ineficaz devido ao grau de complexidade envolvido. Da mesma forma que a política geral de segurança, a política de controle de acesso deve restringir a linhas gerais que cubram a maior parte das situações, deixando as particularidades por conta das exigências dos domínios organizacionais e de recursos que as necessitarem, desde que sigam as diretrizes de grau mais elevado (CARUSO; STEFFEN, 1999).

7 DIREITOS DE ACESSO

De acordo com Beal (2008, p. 71), "as pessoas são, acertadamente, consideradas o "elo frágil" da segurança da informação. A associação pode ser entendida quando se imagina que qualquer esquema de segurança, por mais sofisticado que seja, pode ser derrubado pela atuação de uma única pessoa que decida abusar de seus privilégios de acesso a dados ou instalações de processamento da informação".

Ainda de acordo com Beal (2008, p. 71),

> a melhor política de segurança em relação a qualquer pessoa com acesso aos recursos de informação corporativos continua sendo a descrita pela conhecida expressão *trust, but verify* (confie, mas verifique). Apesar da maior atenção concedida pela mídia aos ataques causados por *hackers*, estudos demonstram que grande parte dos incidentes de segurança é provocada por integrantes da própria organização, sejam eles acidentais (decorrentes de ignorância, erro, negligência ou distração) ou intencionais (por motivo de fraude, vingança, descontentamento etc.). Uma pesquisa global sobre segurança da informação cita diversos estudos para concluir que os incidentes de segurança internos acarretam prejuízos financeiros substancialmente maiores do que os ataques externos.

Quando se fala em "incidentes internos", segundo Beal (2008), é importante considerar também as falhas de segurança provocadas por terceiros com acesso legítimo a recursos de informação da organização: fornecedores, prestadores de serviço, consultores etc. Alguns autores observam que existem consultores que são *hackers* compulsivos, contratados por empresas de segurança justamente pela sua competência em invadir sistemas. Prestadores de serviço também oferecem riscos consideráveis: casos relatados pelos mesmos autores incluem o de um técnico de serviços de campo de uma fabricante de computadores que anotava nas visitas dados como códigos de sistemas de alarme e senhas de abertura de portas para uso futuro em invasões destinadas ao furto de equipamentos – quando os roubos aconteciam, a polícia tinha a impressão de se tratar de trabalho interno, mas ninguém tinha se dado conta de quão "interno" o técnico havia se tornado.

Do ponto de vista da informação baseada em TI, conforme Beal (2008, p. 72), é conveniente analisar os aspectos de segurança relacionados a cada grupo com diferentes níveis de acesso e responsabilidades em relação à manutenção e uso dos sistemas:

7.1 EQUIPE DE SEGURANÇA E ADMINISTRADORES DE SISTEMAS

O bom desempenho do pessoal com atribuições específicas de segurança, incluindo administradores de sistema, é tão importante para a eficácia da segurança da informação quanto aos produtos tecnológicos como *firewall*, ferramentas de criptografia e antivírus. Conhecedores em profundidade das características do ambiente de SI/TI e dos controles estabelecidos, esses profissionais podem provocar consequências desastrosas em caso de desonestidade ou mesmo de desconhecimento ou negligência na realização de suas atividades rotineiras, tais como destruição de dados importantes não protegidos por cópias de segurança ou invasões que poderiam ser evitadas pela instalação de atualizações de segurança em *softwares* críticos (BEAL, 2008).

De acordo com Beal (2008, p. 72), "equipes bem qualificadas, pessoal de reserva para substituição de técnicos em sua ausência, programas de treinamento e supervisão do trabalho são alguns dos principais mecanismos de prevenção contra as ameaças associadas a esse grupo".

7.2 NÚCLEO OPERACIONAL

Conforme Beal (2008), a segurança dos ativos de informação baseados em TI depende da colaboração permanente dos funcionários da organização, que precisam atuar tanto na prevenção (desempenhando as funções de segurança de que foram incumbidos, como, por exemplo, escolher senhas de difícil adivinhação e mantê-las em segredo) quanto na reação a eventuais problemas de segurança (relatando falhas nos controles e incidentes observados). Os procedimentos de segurança de responsabilidade dos usuários finais de sistemas de informação devem estar associados a regras claras, de obediência obrigatória, e a punições em caso de seu descumprimento, e ser adequadamente divulgados para evitar que seu desconhecimento diminua a eficácia dos controles existentes.

Segundo Beal (2008, p. 72),

> os riscos de ataque proposital por parte de integrantes do núcleo operacional devem receber atenção especial por parte da equipe de segurança. Motivos fúteis, como a irritação de um funcionário com o chefe porque ele esqueceu seu aniversário ou escolheu outra pessoa para receber um aumento, podem ser suficientes para desencadear ações prejudiciais à organização, principalmente quando o funcionário tem acesso a uma rede conectada aos mais diversos tipos de serviços e dados corporativos.

De acordo com Beal (2008, p. 73), as principais medidas de segurança a serem adotadas para reduzir os riscos para a disponibilidade, integridade e confidencialidade da informação provocadas pelo elemento humano nas organizações são:

- Processos confiáveis de seleção de pessoal, abrangendo investigação de antecedentes antes da admissão de funcionário ou contratação de temporários e prestadores de serviço.
- Documentação das responsabilidades de segurança nos contratos de trabalho de funcionários e prestadores de serviço, incluindo referência às normas e políticas de segurança da organização às quais os contratados devem se sujeitar.
- Assinatura de acordos de confidencialidade e definição clara de termos e condições de trabalho relativas à segurança da informação, direitos autorais e proteção de dados.

- Supervisão gerencial suficiente para permitir à organização detectar e reagir a situações de risco (como problemas pessoais e financeiros, sinais de estresse etc.) ou atitudes suspeitas (mudanças de comportamento ou de estilo de vida, recusas de tirar férias etc.).

- Nível adequado de segregação de funções, para evitar que uma mesma pessoa se torne responsável por todas as etapas de um processo (por exemplo, controle de todas as atividades relativas à aquisição de bens, da emissão do pedido de compra à confirmação do recebimento).

- Treinamento e conscientização adequada dos funcionários (é comum o pessoal de segurança reclamar da falta de comprometimento dos demais integrantes da organização com as medidas de segurança, mas a ausência de processos eficazes de comunicação dos procedimentos e das razões para sua existência costuma ser a principal razão para o não cumprimento das regras estabelecidas).

- Expectativa de controle e de punição em caso de descumprimento de normas de segurança (os integrantes da organização devem estar cientes dos processos disciplinares e punições a que estarão sujeitos em caso de violação das políticas e procedimentos de segurança e dos mecanismos de controle existentes para detectar essas violações, tais como *logs* gerados para registrar as atividades realizadas pelos usuários dos sistemas).

- Processos seguros de demissão, abrangendo a imediata retirada dos privilégios de acesso físico e lógico aos ativos de informação.

7.3 CÚPULA ESTRATÉGICA E GERÊNCIA INTERMEDIÁRIA

De acordo com Beal (2008, p. 74), dirigentes e gerentes intermediários precisam envolver-se com a implantação dos controles de segurança e comprometer-se com a observância de todos os procedimentos estabelecidos. Se a direção desconsidera normas de segurança, ou permite que subordinados se desviem de determinados controles, todo o esquema de segurança pode ser comprometido. A cúpula estratégica e a gerência intermediária devem procurar identificar os vínculos existentes entre segurança da informação e alcance da missão corporativa, entendendo os custos com segurança como investimentos necessários para se manter no negócio, da mesma forma que os custos com computadores, redes e serviços telefônicos.

> A preocupação com prevenção de atividades ilegítimas, como fraudes, vazamento de informações para concorrentes etc., deve refletir-se em controles destinados a evitar que membros da alta direção ou da gerência média adquiram privilégios excessivos na manipulação de informações ou na realização de atividades críticas nos sistemas corporativos. (BEAL, 2008, p. 74).

7.4 FORNECEDORES, CONSULTORES E PRESTADORES DE SERVIÇO

Segundo Beal (2008, p. 74), fornecedores de bens e serviços, consultores e prestadores de serviço podem representar sérias ameaças à segurança da informação. Principalmente ao terceirizar algum serviço que envolva a manipulação de informações sensíveis e críticas, a organização precisa identificar os riscos envolvidos, e estabelecer não só normas de segurança específicas, mas também processos de aferição da conformidade dos serviços com os padrões de segurança adotados. A ISO 17799 recomenda que seja dada especial importância aos riscos associados ao acesso físico e lógico concedido a prestadores de serviço (item 4.2.1), devendo ser considerada a implantação de controles adicionais nos seguintes casos:

- Equipes de suporte de *hardware* e *software* que precisam utilizar sistemas e aplicações.
- Parceiros comerciais que precisam trocar informações, acessar sistemas ou compartilhar bases de dados.
- Prestadores de serviço que executam serviços internos (como equipes de suporte e manutenção de *hardware* e *software*, pessoal de limpeza, estagiários, consultores etc.).

Os contratos de terceirização ou compartilhamento de informações devem contemplar os requisitos legais e organizacionais de segurança a serem atendidos pelos fornecedores ou parceiros, e explicitar os procedimentos usados para garantir que os envolvidos estejam cientes de suas responsabilidades de segurança. Sempre que possível, os contratos de trabalho dos prestadores de serviço devem registrar as diretrizes e normas de segurança a serem obedecidas. A confiança atribuída a pessoas de fora da organização deve ser baseada em verificações de antecedentes, na obtenção de referências e em verificações rotineiras das atividades desempenhadas (BEAL, 2008).

7.5 ACORDOS DE CONFIDENCIALIDADE

De acordo com Beal (2008, p. 75), "acordos ou contratos de confidencialidade são úteis para alertar empregados e prestadores de serviços sobre os requisitos existentes com relação a informações de caráter sigiloso". A ISO 17799 (item 6.1.3) recomenda que um acordo de confidencialidade seja assinado como parte dos termos e condições iniciais de contratação. Outras responsabilidades de segurança também devem ser registradas em termos e condições de trabalho (item 6.1.4), sendo que os acordos podem prever a continuidade das responsabilidades por um tempo definido após o término do contrato de trabalho e as penalizações cabíveis em caso de desrespeito ao acordo.

7.6 TREINAMENTO DE FUNCIONÁRIOS E PRESTADORES DE SERVIÇO

De acordo com Beal (2008, p. 77), é fundamental para o processo de proteção da informação que os funcionários (e, sempre que cabível, prestadores de serviço) sejam treinados nos procedimentos de segurança, e que todos os usuários do ambiente computacional recebam treinamento quanto ao uso correto dos recursos e instalações de processamento da informação. A ISO 17799 (item 6.2.1) recomenda que sejam feitas atualizações regulares nos treinamentos sobre as diretrizes e os procedimentos organizacionais, incluindo mudanças nos requisitos de segurança, responsabilidades legais e controles do negócio. Funcionários e prestadores de serviço também devem ser informados dos procedimentos para notificação dos diversos tipos de incidente, tais como violação da segurança, ameaças, fragilidades ou mau funcionamento de equipamentos, e os incidentes ocorridos podem ser usados como exemplos em treinamentos para ensinar aos usuários como reagir e evitar recorrências futuras (item 6.3 da norma).

Ainda de acordo com Beal (2008, p. 77), "a organização deve adotar estratégias diversificadas para compor um treinamento e conscientização completos e eficazes, englobando instrumentos complementares, como cursos de capacitação para as equipes técnicas, *workshops*, seminários, campanhas por *e-mail*, cartas da diretoria etc."

7.7 ENGENHARIA SOCIAL

Um aspecto de grande importância e, segundo Beal (2008, p. 78), muitas vezes negligenciado na segurança da informação é a proteção contra ataques de engenharia social. *Hackers* e outros tipos de pessoa mal-intencionada podem valer-se da ingenuidade ou ignorância de usuários para obter informações confidenciais, como senhas, tipos de equipamento de segurança utilizados ou outros dados que podem comprometer a segurança da organização. Um exemplo típico de truque de engenharia social ocorre quando um *hacker* envia um *e-mail* para um usuário, apresentando-se como administrador da rede corporativa, e solicita a entrega da senha para a realização de alguma tarefa de suporte ou de manutenção dos serviços. A mensagem é enviada para um grande número de usuários, na esperança de que um ou dois acabem sendo enganados.

Conforme Beal (2008), muitos *hackers* bem-sucedidos na invasão de sistemas, ao serem entrevistados, admitem ter obtido senhas e outras informações que possibilitaram o ataque pelo uso de engenharia social. Há casos em que o invasor simplesmente postou-se na frente do portão de entrada de uma empresa e, fazendo-se passar por estudante realizando um trabalho de escola, conseguiu extrair de funcionários as senhas por eles usadas para acessar sistemas corporativos. A recusa na prestação de informações sobre a senha pessoal e outras informações privilegiadas a quem quer que seja (incluindo colegas de trabalho), o bloqueio da visão de terceiros do teclado quando da digitação da senha e a confirmação

da procedência de mensagens suspeitas antes da realização de qualquer ação solicitada por *e-mail* são orientações que devem constar nos programas de treinamento e conscientização dos usuários para diminuir os riscos associados à engenharia social.

7.8 SEGREGAÇÃO DE FUNÇÕES

A segregação de funções, de acordo com Beal (2008, p. 79),

> é um controle essencial para a redução dos riscos para a segurança da informação. A separação das responsabilidades relativas a diferentes etapas de um processo reduz as oportunidades de uso indevido dos recursos de informação e ajuda a prevenir a ocorrência de fraudes, obrigando a existência de cumplicidade para concretizar o dano. A preocupação com a segregação de funções deve abranger todas as áreas de risco, das operações de TI aos processos de aquisição, pagamento, controle de estoques etc.

"A ISO 17799 (item 8.1.4) sugere, nos casos em que for difícil implementar a segregação de funções, que outros controles, como a monitoração das atividades, trilhas de auditoria e supervisão gerencial, sejam considerados para diminuir a vulnerabilidade da organização". (BEAL, 2008, p. 79).

7.9 PROCESSO DISCIPLINAR

Segundo Beal (2008, p. 79), "a organização precisa dispor de um processo disciplinar aplicável a pessoas que tenham violado políticas ou procedimentos de segurança. A expectativa de punição é essencial para ajudar a inibir comportamentos que podem acarretar desrespeito às normas de segurança".

RESUMO DO TÓPICO 1

Caro(a) acadêmico(a)! Neste primeiro tópico, você estudou os seguintes aspectos:

- Os principais conceitos no que tange à segurança da informação em um ambiente computacional.
- O ciclo de vida da informação dentro de uma organização.
- A segurança da informação baseada em modelos tradicionais e computacionais.
- Como diminuir os riscos, vulnerabilidades e as ameaças inerentes ao sistema de informação através de medidas de segurança, que garantirão a proteção dos ativos.
- A análise dos possíveis riscos e como realizar o tratamento dos mesmos.
- A classificação das informações em variados níveis, segundo o seu grau de importância.
- As formas de armazenamento e descarte das informações.
- O direito de acesso às informações e suas formas de controle.
- A análise de diversos aspectos da segurança da informação no contexto físico, lógico e ambiental.
- Os diversos recursos implementados a fim de garantir a segurança da informação nos sistemas distribuídos.

AUTOATIVIDADE

1 Com o intuito de garantir a disponibilidade da informação no ambiente computacional, o usuário poderá realizar *backup* (cópia de segurança) dos arquivos com informações relevantes em mídias e locais diferentes.

( ) CERTO.
( ) ERRADO.

2 Conforme os estudos realizados, verificou-se que a segurança de recursos de informação possui três componentes, integridade, disponibilidade e confidencialidade. Com relação aos componentes citados, assinale a opção CORRETA:

a) ( ) A integridade pode ser obtida a partir do momento em que existe confidencialidade.
b) ( ) A integridade estabelece que, a informação somente será liberada para usuários legítimos.
c) ( ) O nível de segurança pode ser elevado ao aditar a integridade a um sistema com confidencialidade.
d) ( ) A confidencialidade tem por objetivo garantir que, a informação seja verdadeira, completa e precisa.

Assista ao vídeo de resolução da questão 2

TÓPICO 2

SEGURANÇA LÓGICA, FÍSICA E AMBIENTAL

1 INTRODUÇÃO

Os problemas de segurança da informação são complexos, conforme Beal (2008), e normalmente têm sua origem em preocupações organizacionais e de negócio, não de tecnologia. Para garantir um nível de proteção adequado para seus recursos de informação, as organizações precisam ter uma visão clara dos ativos que estão tentando salvaguardar, de que ameaças e por que razão, antes de poder passar à seleção de soluções específicas de segurança física, lógica e organizacional.

O propósito deste tópico é demonstrar uma visão da segurança da informação em todos os contextos, de segurança lógica, física e ambiental, de modo a permitir o desenvolvimento e implantação de medidas de segurança que possam proteger as organizações, os geradores das informações e os seus usuários, dos inúmeros danos que podem ser causados por conta da destruição, acesso, alteração, exclusão ou divulgação indevida destas informações, causando sérios prejuízos financeiros, perda de credibilidade no mercado, desvalorização das ações da organização, danos à imagem da corporação ou ainda sanções e penalizações por conta do descumprimento de leis ou cláusulas contratuais de confidencialidade, entre tantas outras.

2 SEGURANÇA LÓGICA

É desnecessário justificar as demandas de segurança nas instalações de Tecnologia da Informação. As informações de uma empresa têm valor não só para ela, como também para seus concorrentes (espionagem empresarial) e para outras empresas (cadastros de clientes, lista de produtos etc.). A preocupação com a segurança das informações da empresa deve ser uma constante em todos os setores, principalmente na área de Tecnologia de Informação (FOINA, 2009).

De acordo com Foina (2009, p. 179), "pela área de Tecnologia de Informação transita grande número de informações sensíveis e estratégicas para a empresa (e de interesse de outras empresas, concorrentes ou não)". A divulgação de algumas dessas informações pode ocasionar prejuízos e penalidades graves (mais um motivo para que a segurança da área seja preocupação constante de seus executivos).

Foina (2009, p. 180) cita que "a segurança lógica compreende a integridade dos ativos de dados e dos programas da empresa. Uma sabotagem nos arquivos de dados pode provocar a paralisação da empresa por um período significativo, prejudicando sua imagem junto ao mercado".

2.1 ASPECTOS GERAIS DA SEGURANÇA LÓGICA

No ambiente atual de interligação de redes, de acordo com Beal (2008, p. 91),

> os problemas de segurança se multiplicam de forma alarmante. Nos dias de hoje, qualquer usuário com um microcomputador ou *laptop* se transforma num "administrador de sistema", precisando gerenciar localmente uma série de procedimentos de segurança, como ferramentas antivírus, opções de segurança do navegador de internet, etc. Isso significa que basta um único usuário não estar vigilante para que toda rede esteja vulnerável a um problema (por exemplo, a contaminação por vírus). No caso de uma rede conectada à Internet, a mera segurança física dos equipamentos conectados já não garante nenhuma proteção: os recursos da rede deixam de estar num endereço físico fixo para pertencer ao chamado "ciberespaço", ambiente virtual criado pela rede mundial de computadores, e precisam ser protegidos contra quebras de segurança causadas por ameaças externas (invasões, ataques de negação de serviço, etc.) e internas (erros, abusos de privilégio, fraudes, etc.).

Foina (2009, p. 180) cita que

> a segurança lógica trabalha estabelecendo mecanismos de acesso a arquivos, sistemas e páginas *Web* da empresa, limitando a disponibilidade de recursos para cada usuário. Um bom sistema de controle de acesso permite identificar tentativas de quebras de segurança antes de se efetivem (detecção de intruso). Mesmo havendo quebra de segurança, permitem rastrear a origem da violação e os efeitos causados sobre os arquivos (rastreabilidade).

2.2 ADMINISTRAÇÃO DA SEGURANÇA

O passo seguinte na implantação da estrutura de segurança, logo após a definição das diretrizes da política de segurança, é a definição da estrutura da administração de segurança. Devem ser considerados aspectos como estrutura da administração de segurança, tipo de estrutura, sua localização dentro da estrutura da organização, perfil exigido do profissional que exercerá a função do administrador de segurança, diretrizes da segurança, ferramental administrativo e técnico utilizado, equipe de projeto incumbida de implementar a segurança, grau de padronização exigido etc. (CARUSO; STEFFEN, 1999).

De acordo com Caruso e Steffen (1999, p. 105), "mesmo que a estrutura da administração de segurança possua seu foco na segurança do acesso lógico, essa área também deverá ser a responsável, ao menos em nível normativo, pela segurança física dos ambientes de informações".

2.2.1 A estrutura da administração da segurança

Uma das primeiras coisas a ser considerada após a definição das diretrizes é a estrutura da administração de segurança. Deve ser montada uma estrutura que, ao final da implantação do projeto de segurança assumirá as tarefas normais de administração de segurança do ambiente de informações, tanto no aspecto físico como no aspecto lógico, definindo claramente o seu domínio de atuação, a autoridade e as regras sobre as quais se basearão suas atividades.

Ainda que esse tipo de estrutura se aplique a qualquer organização ela está mais relacionada com ambientes de informações baseados em facilidades de informática.

2.2.2 Tipos de estruturas

Segundo Caruso e Steffen (1999, p. 106), "deve-se definir o tipo de estrutura de administração da segurança entre centralizada ou descentralizada". Para os dois tipos de estrutura existem tanto argumentos válidos, não existindo uma resposta pronta e certa para se tomar essa decisão. Pode existir uma resposta certa em relação a um ambiente individual, mas somente uma cuidadosa análise de cada ambiente de informações pode determinar qual será a melhor resposta.

A seguir serão listados alguns pontos que devem ser considerados no processo de tomada de decisão quanto ao tipo de estrutura.

De acordo com os autores Caruso e Steffen (1999, p. 106), "segurança centralizada proporciona um controle mais eficiente em relação às mudanças na segurança e possivelmente nos trabalhos para se impor a segurança. Porém o esforço de manutenção da segurança nesse nível pode ser necessário o gerenciamento de uma equipe considerável". No quadro a seguir são identificadas as vantagens e desvantagens da centralização da segurança.

QUADRO 8 – VANTAGENS E DESVANTAGENS DA CENTRALIZAÇÃO

Vantagens	Desvantagens
Maior simplificação organizacional e de procedimentos.	Menor grau de flexibilidade.
Especialistas de segurança dedicados.	Desconhecimento de condições locais.
Menor dispersão de esforços.	Custo maior concentrado em uma única área.
Menor sobreposição de estruturas de segurança.	Tempo de resposta mais lento.
Maior rapidez de manutenção.	

FONTE: Adaptado de Caruso e Steffen (1999, p. 107)

Ainda de acordo com Caruso e Steffen (1999, p. 106),

> a segurança descentralizada distribui o esforço de manutenção da segurança, de forma que a função não se torne um ônus para apenas uma área. Além disso, a manutenção poderá ser subordinada a uma área que pode ter um conhecimento maior e mais adequado dos recursos que serão protegidos. Porém, haverá um esforço adicional na área central para controlar as atividades dos administradores descentralizados.

No quadro a seguir são mostradas as vantagens e desvantagens da descentralização.

QUADRO 9 – VANTAGENS E DESVANTAGENS DA DESCENTRALIZAÇÃO

Vantagens	Desvantagens
Maior flexibilidade.	Aumento da burocracia.
Manutenção local mais rápida.	Maior sobreposição de estruturas de segurança.
Maior familiaridade com as exigências locais.	Menor conhecimento da segurança.
Responsabilidade e relacionamento distribuídos.	Maior suscetibilidade a pressões locais.
	Maiores dificuldades de controle por parte da auditoria ou outro órgão de controle.

FONTE: Adaptado de Caruso e Steffen (1999, p. 108)

Para Caruso e Steffen (1999, p. 106), é necessário levar em consideração alguns aspectos para decidir quem deve ser o responsável pela administração da segurança, como o tamanho de cada organização, as instalações de processamento de informações da empresa e das atividades de manutenção necessárias e isto dependerá dos seguintes aspectos:

- Do número de entidades hierárquicas e ferramentas envolvidas, ou seja, departamentos, divisões, aplicações etc.

- Do número de usuários definidos, e dos requisitos de movimentação de empregados.
- Da quantidade de recursos que devem ser protegidos.
- Da existência de padrões.
- Dos diferentes tipos de recursos que devem ser protegidos e da extensão da segurança requerida para cada um destes recursos. Deve ser lembrado que a Internet pode exigir uma estrutura exclusiva de controle.
- Do número de entidades que devem ser protegidas, o que pode implicar um trabalho de manutenção enorme em alguns casos.
- Das atividades de desenvolvimento de aplicações. Se a atividade de desenvolvimento for considerável, como é o caso da maioria das instalações, a revisão da segurança e das atividades de manutenção também devem ser consideradas.
- Dos requisitos de auditoria e da frequência de alterações destas.
- Do número de recursos definidos para os usuários e das atividades previstas para eles.
- Das ferramentas de segurança selecionadas. Cada uma difere das outras em função do volume de trabalho envolvido e do perfil necessário para a manutenção da segurança.

Muitas organizações, segundo Caruso e Steffen (1999, p. 107), "utilizam no início a administração centralizada e posteriormente, descentralizam a função quando os requisitos de manutenção se tornem práticos". Normalmente, essa é uma abordagem inicial mais racional, já que permite que a equipe do nível central se torne perita em segurança antes que seja necessário treinar e controlar administrados e equipes em um nível descentralizado.

2.2.3 Localização da segurança

Uma das primeiras questões a serem consideradas, segundo Caruso e Steffen (1999, p. 108), "é a localização da segurança". Segundo eles, é melhor que o administrador de segurança esteja envolvido desde o início da implantação da estrutura de segurança. Dessa forma, o administrador será capaz de gerenciar as tarefas diárias e constantes.

A função de um administrador de segurança deve residir em algum lugar dentro da própria organização. Para Caruso e Steffen (1999, p. 108), o melhor lugar é onde a área de administração de segurança se relacione mais diretamente com a alta administração. Isso é necessário para que a área se torne menos suscetível a pressões e comprometimentos resultantes de lealdades para com a área funcional à qual a administração de segurança pertença. Também, em alguns casos, pode

ser vantajoso incluir todas as funções de segurança, compreendendo os requisitos de segurança física, dentro desta área. Isso segue a clássica abordagem de agrupamento de funções similares de modo que se evite a existência de estruturas similares dentro da organização.

Porém, o custo de uma estrutura pode ser muito alto para as organizações. Neste caso, segundo Caruso e Steffen (1999, p. 108), a administração de segurança deve residir em uma área onde tenha o poder de impor a segurança. Esse poder deve ser formalmente garantido e apoiado ativamente pela alta direção. Esta área deve ter também a mão de obra necessária para preencher as funções. Se possuir estas características, a administração de segurança pode residir em qualquer lugar dentro da organização.

Utilizando uma analogia do cenário acima com o ditado de "colocar a raposa para tomar conta do galinheiro", nos indica que, de acordo com Caruso e Steffen (1999, p. 109), "não se deve conectar a administração de segurança a nenhuma das funções de informática, pois elas também são usuárias da segurança". A área de auditoria também não pode ser ligada a administração da segurança, pois cabe a ela fiscalizar esta área.

É conveniente que a definição da estrutura de segurança conste da política de segurança, ao menos em suas linhas gerais. Caruso e Steffen (1999, p. 109) "indicam que bom é posicioná-la, pelo menos em termos de subordinação hierárquica, junto à estrutura de segurança empresarial, que cuida da segurança das organizações em um nível global, caso exista tal estrutura dentro da empresa". Como várias outras estruturas nas organizações, este tipo de estrutura está diretamente vinculada ao porte de cada organização.

Contudo, a centralização proposta não significa a centralização operacional. Para Caruso e Steffen (1999, p. 109), "as organizações devem ter uma política de segurança global, voltada para a normatização e o controle. Essa normatização e controle não significam a centralização operacional".

2.2.4 Perfil do profissional de segurança

Após a definição do posicionamento da administração de segurança, segundo Caruso e Steffen (1999, p. 109), "a próxima etapa é decidir quem irá preencher a função". O trabalho de um administrador de segurança é, sem dúvida, difícil. A natureza da função forçará o administrador a se imiscuir em todos os "cantos escuros" da organização. Além disso, é uma posição de alta responsabilidade, que requer determinação e segurança por parte do profissional. Entre as diversas características que um administrador de segurança em potência, de acordo com Caruso e Steffen (1999, p. 109), deve possuir:

- Conhecimento dos recursos dos ambientes de informações e dos requisitos de segurança adequados.
- Alto grau de responsabilidade.
- Boa experiência organizacional e em análises.

- Sensibilidade para a política do ambiente de informações.
- Facilidade em se relacionar, pois a maior parte do trabalho envolve convencer as pessoas.
- Estabilidade emocional.

Manda a prudência que seja definido um substituto para o administrador de segurança desde o início, de maneira que a função possa continuar se, por qualquer motivo, o administrador de segurança inicialmente selecionado não puder. Para Caruso e Steffen (1999, p. 109), essa sugestão segue a clássica abordagem de que "ninguém é mais insubstituível ou eterno".

Além disso, pode ser necessária uma equipe de apoio. Esta equipe deve ser composta por analistas de segurança e apoio administrativo e do administrador de segurança.

Diz-se que um bom profissional de segurança deve ter coração de pedra e nervos de aço e ser insensível a ofensas e insultos. (CARUSO; STEFFEN, 1999, p. 110).

2.2.5 Diretrizes da segurança

As diretrizes que governarão a segurança devem ser definidas logo no início. Segundo Caruso e Steffen (1999, p. 110), o ideal é que elas já estejam definidas na política global de segurança da empresa, como parte das atribuições e responsabilidades que se espera que todos os empregados sigam. As diretrizes de segurança mais específicas devem ser formadas de normas à parte da política e devem se basear nas diretrizes gerais da política, porém não devem ser rígidas para que seja possível adequar às particularidades de cada caso.

Quando falamos de diretrizes, entendem-se as regras gerais que orientarão a elaboração de normas e procedimentos subordinados à política de segurança. De acordo com Caruso e Steffen (1999, p. 110), em princípio, as diretrizes de segurança devem contemplar os seguintes aspectos:

- Procedimentos padrões de segurança que serão utilizados no ambiente de trabalho na empresa.
- Documentação dos controles de segurança disponíveis para cada tipo de recurso e a comunicação a todos os envolvidos.
- Estimativa dos riscos e comprometimentos dentro do ambiente da empresa.

- Registro e relato das violações para as pessoas indicadas.
- Acompanhamento do desenvolvimento de requisitos de segurança para todos os projetos dos usuários.
- Treinamento de todos os usuários com relação à política de segurança da empresa.
- Se for necessário, apoio às administrações descentralizadas e seu controle.
- Responsabilização dos envolvidos com a função de segurança, desde o administrador central até o usuário final; deve ser dado um enfoque especial ao papel das áreas de informática em relação à segurança, já que é ali que se encontram as maiores vulnerabilidades.

2.2.6 Ferramental administrativo e técnico

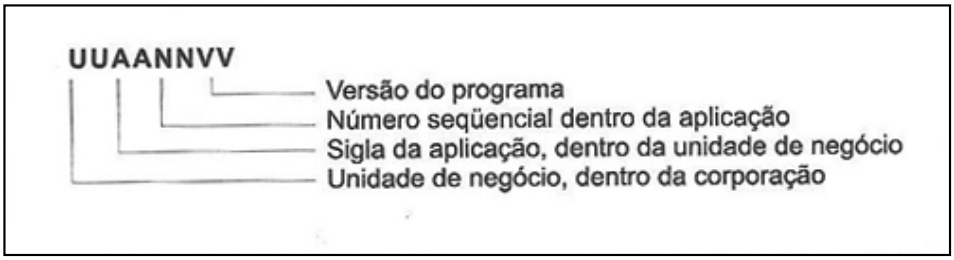
Seguindo a linha de raciocínio de Caruso e Steffen (1999, p. 111), o próximo passo é definir as ferramentas administrativas e técnicas relacionadas com a função de segurança. Uma boa parte dos procedimentos administrativos depende da definição de outros aspectos da segurança, como diretrizes globais e específicas da segurança, a estrutura e o tipo de estrutura utilizados, o tamanho da equipe, o produto de segurança a ser adotado, entre outros. O ferramental administrativo é altamente dependente da cultura de cada organização enquanto que o ferramental técnico é dependente do produto de segurança adotado pela empresa.

2.2.7 Padronização

Padronização de nomenclatura é o tipo de atividade que todos acham necessária, mas que, frequentemente, vai sendo adiada indefinidamente. Para Caruso e Steffen (1999, p. 111), "se a organização conseguiu desenvolver padrões válidos em nível global antes da implantação da segurança, será muito mais fácil padronizar as nomenclaturas, já que os produtos de segurança são baseados, em grande parte, no agrupamento de funções de segurança".

Se já existem padrões de nomes, de acordo com Caruso e Steffen (1999, p. 111), "a definição de listas de acesso torna-se mais fácil, devido ao agrupamento permitido pelo uso de qualificadores de nomes de nível mais geral". Na figura a seguir damos um exemplo para dar nomes a programas em uma organização com uma estrutura baseada em centros de lucro ou unidades de negócio.

FIGURA 9 – EXEMPLO DE PADRÃO DE NOMENCLATURA DE PROGRAMAS



FONTE: Caruso e Steffen (1999, p. 111)

Entretanto, ainda segundo Caruso e Steffen (1999, p. 112), se você está em uma das muitas organizações que não possuem padrões ou que sua aplicação não seja geral, a implantação será um pouco mais complicada, já que a padronização será necessária para a maioria das definições de recursos para o pacote de segurança.

Caruso e Steffen (1999) citam que o volume de manutenção exigido por uma estrutura de segurança é inversamente proporcional ao grau de padronização existente dentro da organização. Quanto maior esse grau, menor o volume de manutenção e vice-versa.

É conveniente observar que a implantação da segurança será uma boa ocasião para desenvolver e implantar padrões de nomenclatura de recursos, tão importantes em cada organização. O produto de segurança pode ser muito útil na imposição desses padrões. Quando o inventário tiver sido completado e você estiver familiarizado a respeito do que a organização possui e quem é responsável por quais elementos, poderá ser a ocasião adequada para projetar padrões ou planejar seriamente a imposição de padrões projetados, mas nunca usados com sucesso. A maior parte dos produtos de segurança pode ser usada de tal maneira que a maioria dos usuários terá permissão para ler ou atualizar recursos de uso corrente que não estejam dentro dos padrões, mas não terá permissão para criar recursos que desobedeçam aos mesmos (CARUSO; STEFFEN, 1999).

De acordo com Caruso e Steffen (1999, p. 112), "os produtos de segurança normalmente permitem o uso de nomes definidos por usuários para nomear entidades funcionais dentro do banco de dados de segurança. Os nomes usados dentro deste banco também devem seguir um padrão para simplificar as manutenções e permitir facilmente pesquisas e análises".

2.2.8 Equipe do projeto

Nesta fase, conforme Caruso e Steffen (1999, p. 112), "a equipe de implantação do projeto deve estar constituída, ou pelo menos devem estar descritas as diretrizes que governarão o trabalho da equipe". O administrador de segurança, que já deve estar definido a esta altura, deve ser o coordenador da equipe. Se a estrutura da administração de segurança já tiver sido implantada, é conveniente que pelo menos um dos integrantes participe da equipe, de preferência na função de relator e para providenciar os trâmites administrativos necessários.

2.2.9 Controles

Algumas atividades administrativas necessitam de controles firmes, e segurança de informações é uma delas. É necessário controlar o domínio de usuários, o domínio de recursos e as interações entre os dois domínios. A esta altura da montagem da estrutura de segurança devem ser definidos os controles desejados que serão implantados após a escolha da ferramenta de segurança. Muitos pacotes de controle de rede também possuem recursos de segurança embutidos, apesar de

nem todos serem tão completos quanto as ferramentas dedicadas exclusivamente à segurança (CARUSO; STEFFEN, 1999).

De acordo com Caruso e Steffen (1999, p. 113),

> todos os pacotes de segurança dispõem de recursos de emissão de relatórios sobre a estrutura da segurança e das atividades dos usuários. Mas nem todos permitem a formatação dos dados de forma livre, nem a inserção de títulos em língua diferente do país de origem. Caso os mesmos não se revelem adequados à sua organização, é necessário desenvolver programas específicos. Algumas ferramentas de segurança permitem selecionar registros para um arquivo intermediário, usado como entrada para programas personalizados. Informações sobre a estrutura da segurança, com os dados sobre usuários, recursos e interações entre os mesmos, acham-se gravadas no banco de dados do pacote de segurança escolhido. Dados das atividades de usuários são normalmente gravados nos arquivos de registro de atividades do sistema operacional ou dos pacotes de *software*; alguns deles permitem a opção de gravar esses dados também em mais de um arquivo, podendo também ser acessados em tempo real.

Normalmente, segundo Caruso e Steffen (1999, p. 113), "serão necessários relatórios de controle de dois tipos: controle da estrutura de segurança e controle sobre atividades de usuários".

2.2.9.1 Controle da estrutura de segurança

Caruso e Steffen (1999, p. 113) afirmam que, basicamente, os relatórios de controle da estrutura destinam-se a controlar os usuários, os recursos e as interações entre usuários e recursos.

a) Usuários e grupos de usuários:

- Estrutura hierárquica dos grupos de usuários.
- Usuários de cada grupo.
- Usuários com atributos especiais.

b) Recursos:
- Grupos de recursos protegidos.
- Recursos de cada grupo.
- Nível de proteção de cada grupo de recurso.
- Nível de proteção de cada recurso individual.
- Recursos com proteção especial.

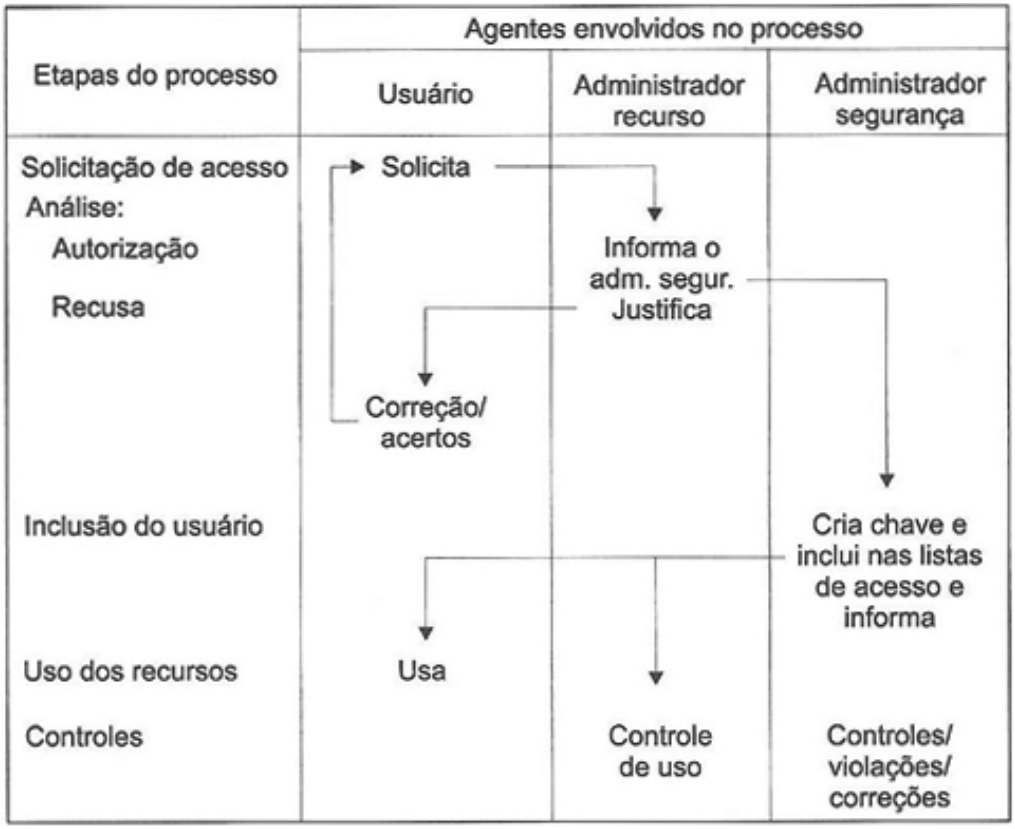
c) Interações usuários versus recursos:
- Recurso que cada usuário pode acessar.
- Usuários que acessam cada recurso.
- Nível de acesso permitido a cada grupo / usuário.

2.2.9.2 Controle sobre atividades de usuários

Basicamente, conforme Caruso e Steffen (1999, p. 114), os relatórios de controle de atividades de usuários destinam-se a controlar a forma como os usuários fazem uso dos recursos que lhes são disponibilizados e as violações que os mesmos cometem.

- Violações de acesso a ambientes.
- Violações de acesso a recursos.
- Acesso a recursos monitorados.
- Acesso de usuários monitorados.

FIGURA 10 – FLUXO ADMINISTRATIVO DA CONCESSÃO DE ACESSO A UM RECURSO CONTROLADO



FONTE: Caruso e Steffen (1999, p. 111)

A lista de relatórios acima é apenas uma sugestão; cada ambiente deve estabelecer sua própria lista, em função de suas particularidades. Além dos relatórios acima, relacionados com a ferramenta de segurança, existem outros que podem ser montados e que não estão relacionados com essa ferramenta. É o caso do relatório de movimentação de pessoal ou do relatório de funcionários demitidos, essenciais para determinar direitos de acesso e que devem ser fornecidos pela área de recursos humanos. Entretanto, tal tipo de informações pode vir a exigir alterações nos bancos de dados da área de recursos humanos para se introduzirem informações relacionadas com o acesso aos ambientes de informações (CARUSO; STEFFEN, 1999).

2.3 DEFINIÇÃO DA EQUIPE

De acordo com Caruso e Steffen (1999, p. 118), a equipe do projeto deve ser composta por elementos oriundos das áreas que serão mais afetadas pela estrutura de segurança. A medida se prende ao fato de se ter que atender aos requisitos de segurança de todos os envolvidos. O propósito básico desse envolvimento é desenvolver um sentimento de participação e de responsabilização conjunta no produto final da segurança.

FIGURA 11 – MODELO DE ESTRUTURA DE EQUIPE PARA PROJETO DE SEGURANÇA DE ACESSO LÓGICO

FONTE: Caruso e Steffen (1999, p. 121)

Na figura 11 é mostrado um modelo de estrutura da equipe do projeto de segurança de acesso. Caruso e Steffen (1999, p. 118) lembram que o tamanho da equipe depende do próprio tamanho da organização e dos equipamentos – variedade, quantidade e porte – usados dentro da mesma. Em princípio, ainda segundo os autores, a equipe do projeto deve ser composta com elementos das seguintes áreas:

- Administração de segurança – a esta altura o administrador de segurança já deve ter sido escolhido; a função dele na equipe do projeto é a coordenação do projeto. Além do administrador de segurança, podem-se alocar mais elementos da equipe de segurança – se a estrutura já estiver montada – para assessorar a equipe e executar as tarefas operacionais exigidas pela implantação.
- *Software* básico e de apoio – esta área é a responsável técnica, dentro da maioria das organizações, pelo ferramental de informática utilizado para processar e armazenar informações. A esta área caberá a implantação da ferramenta de segurança e sua adaptação ao ambiente operacional da organização. Esta área faz uso de recursos que, frequentemente, contornam a segurança ou então propiciam o desenvolvimento de brechas na segurança. Além disso, muitas das diretrizes básicas de informática e de processamento de informações emanam desta área, de modo que sua participação é imprescindível. Nem todas as organizações dispõem de uma área que cuide especificamente do *software* básico; além disso, é muito frequente que, mesmo em grandes organizações, as áreas de *software* básico e de apoio também tenham responsabilidade sobre bancos de dados. Em microinformática, é muito comum que as funções de *software* básico e administração de dados sejam exercidas por pessoas alocadas na mesma função.
- Administração de dados – esta área é responsável pela administração dos ativos de informação residentes nos computadores, pela operacionalização e pelo uso dos *softwares* de banco de dados e pela integridade dos ativos de informação residentes em bancos de dados. A maioria dos desvios de uso de ativos das organizações ocorre em cima de informações armazenadas em bancos de dados. Como, além disso, normalmente esta área também tem a responsabilidade pelas normas de nomes de arquivos, sua participação é indispensável.
- Produção – em organizações com processamento de informações centralizado, esta área é a responsável pelo processamento de todos os serviços de informática. Em organizações que fazem uso de recursos de diversas redes de microcomputadores centralizadas, frequentemente há uma área central responsável pela produção. Quando não houver, isso passa a ser um problema departamental. Como nessas organizações esta área é a que está em contato mais direto com os usuários, ela é geralmente afetada pelas medidas de segurança, à medida que tiver de administrar os requisitos de segurança de acesso de usuários aos computadores. Além disso, ela também é a custodiante dos ativos de informação e, portanto, talvez a mais interessada na preservação da integridade dos ativos sobre os quais tem responsabilidade. Em microinformática, normalmente esta função é de responsabilidade da área de teleinformática.
- Comunicação de dados e redes – atualmente, grande parte do processamento de informações envolve linhas de comunicação. Esta área também é grandemente afetada pelas medidas de segurança, pois a grande maioria dos acessos de usuários aos sistemas computadorizados envolve comunicação de dados. Os principais riscos corridos pelos ativos de informação estão justamente nas linhas de comunicação, muito sujeitas à interceptação. Além disso, as áreas envolvidas em comunicação de dados

têm requisitos de segurança próprios que devem ser levados em conta. Em microinformática, normalmente esta função é de responsabilidade das áreas usuárias. É fundamental que alguém dentro da equipe conheça a fundo a internet e seu ferramental; cada vez mais o processamento de informações tende a ser feito através da internet. Quando chegar a hora de conectar seus equipamentos ou sua rede interna à internet, isso deve ser feito com pleno conhecimento de causa.

- Desenvolvimento de aplicações – ainda que em muitas empresas esta área esteja diminuindo de tamanho, com a devolução de atividades para as áreas afins, ela permanece como o centro focal das atividades de desenvolvimento de aplicações, desenvolvendo-as para áreas que não tenham estrutura suficiente para possuir uma área de desenvolvimento autônoma e normatizando as atividades de desenvolvimento de aplicações. Além disso, na maioria das organizações, essa área é a responsável pelos recursos de desenvolvimento de aplicações, como bibliotecas de linguagens e demais ferramentas, normatização etc. Também é recomendável que a área de desenvolvimento seja a responsável pelo estabelecimento de um padrão único de segurança de aplicativos, para que todos se encaixem no mesmo. Dessa forma, evita-se a duplicidade de esforços, já que é comum cada equipe de desenvolvimento de aplicações desenvolver sua própria segurança interna. Uma das vantagens dessa abordagem é o aumento da produtividade. Em microinformática, normalmente esta função é de responsabilidade das áreas usuárias ou de suporte ao usuário.
- Auditoria – em todas as empresas onde exista uma área específica de auditoria, seu papel é controlar o uso dos ativos da organização em nome dos legítimos proprietários. Portanto, ela deve controlar a adesão das partes às normas e procedimentos estabelecidos. Na equipe do projeto, seu papel é garantir que o processo da implantação de segurança e as próprias diretrizes de segurança sigam as diretrizes globais da organização.
- Usuários – as atividades de processamento de informações existem em função dos usuários. Portanto, nada mais justo que os mesmos também tenham papel ativo na implantação da segurança. A segurança deve garantir a integridade dos ativos da empresa, mas não deve em hipótese alguma acarretar transtornos para os usuários finais. A dificuldade de se selecionar um representante legítimo dos usuários não deve impedir que os mesmos participem da implantação do projeto de segurança. Se a individualização de representantes de usuários for muito difícil, uma alternativa será convocar um representante de cada uma das grandes funções dentro da organização para que constituam um grupo à parte, ao qual serão reportadas todas as medidas que impliquem a participação de usuários e que deverá ser consultado acerca de necessidades específicas dos usuários.
- Treinamento – a implantação da segurança implica grande trabalho de treinamento dentro da organização, relacionado com os requisitos da segurança. Por esse motivo, mesmo que um representante dessa área não participe da equipe, ou que a organização não possua uma área de treinamento específica, é conveniente que a equipe do projeto conte com assessoria de pessoal especializado em treinamento. Deve-se lembrar que, mesmo após o encerramento do projeto, a estrutura da segurança continuará a existir; todas as atividades de treinamento de novos funcionários e a reciclagem de treinamento competirão a esta área. Se nenhum representante

dessa área participar da equipe, é conveniente ao menos que todos os requisitos de treinamento sejam submetidos à sua apreciação.
- Atividades de apoio – mesmo que o projeto de segurança não implique muitas atividades extras, não relacionadas diretamente com atividades ligadas a informações, podem existir situações em que se precise de assessoria de funções como administração patrimonial, transportes, comunicações etc. Mesmo que estas áreas não participem diretamente do projeto, é conveniente que acompanhem o desenvolvimento do mesmo e que forneçam consultoria e apoio técnico e administrativo relacionados com suas áreas de conhecimento.
- Consultoria externa – embora o maior volume dos esforços de implantação de um projeto de segurança recaia sobre os membros da equipe pertencentes à organização, é conveniente prever a necessidade de consultoria externa da empresa fornecedora dos equipamentos, de consultores de segurança, de fornecedores de ferramentas de segurança etc. Ainda que a estrutura final da segurança seja altamente dependente da própria cultura da organização, muitas questões relacionadas com segurança exigirão apoio externo para tecnologia não disponível internamente ou que não comporte o desenvolvimento interno. Dessa forma, pode-se adquirir muito conhecimento tecnológico útil para a organização.

Em organizações de menor porte, ou mesmo de grande, e com processamento de informações distribuído, conforme Caruso e Steffen (1999, p. 121), "as funções de produção, comunicação de dados e desenvolvimento de aplicativos ou estão frequentemente subordinadas às áreas usuárias ou são cumulativas".

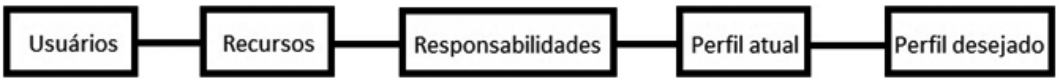
2.4 LEVANTAMENTO DE RECURSOS E DE USUÁRIOS

A tarefa mais trabalhosa na implantação da segurança em uma organização pode vir a ser o inventário de usuários e recursos. O volume de trabalho envolvido dependerá em grande parte do grau de padronização de nomenclatura (nomes de programas, arquivos, transações, chaves de acesso etc.) e da ordem já existente na organização. Uma empresa sem um padrão único, ou desorganizado, requererá mais trabalho de levantamento (CARUSO; STEFFEN, 1999).

No inventário, segundo Caruso e Steffen (1999, p. 126), devem ser levadas em conta as necessidades de cada grupo de usuários; se possível, o inventário deve ser efetuado pelos proprietários dos recursos que estão sendo inventariados. Entretanto, a metodologia deve ser única e ser desenvolvida ou aprovada pela equipe do projeto. O inventário deve responder às seguintes questões:

- Quem são os usuários?
- Quais são os recursos e como eles podem ser classificados?
- Quem é o responsável por cada recurso?
- Qual é o perfil atual de acesso a recursos?
- Qual é o perfil desejável de acesso a recursos?

FIGURA 12 – ETAPAS DE UM INVENTÁRIO DE USUÁRIOS E RECURSOS E SUAS INTERAÇÕES



FONTE: Caruso e Steffen (1999, p. 127)

2.5 SELEÇÃO E ESCOLHA DAS FERRAMENTAS DE SEGURANÇA

Da mesma forma como os procedimentos de segurança refletem as linhas da política de segurança, de acordo com Caruso e Steffen (1999, p. 135), as ferramentas de segurança escolhidas para monitorar e controlar os acessos a ambientes de informações residentes em computadores devem seguir os procedimentos que foram desenvolvidos com base na política de segurança.

Antes mesmo da escolha das ferramentas de segurança, conforme Caruso e Steffen (1999, p. 135),

> deve-se ter conhecimento do ambiente global a ser protegido. Esse conhecimento irá permitir a definição dos quesitos para a avaliação dos produtos disponíveis. A implantação da segurança em um ambiente computacional é, antes de tudo, uma tarefa administrativa; portanto, deve-se ter sempre em mente que o ferramental técnico é um meio e não um fim em si mesmo. Dessa forma, as ferramentas de segurança escolhidas devem se adaptar ao ambiente que vão proteger e não o contrário. Quanto mais aspectos do ambiente forem cobertos pela ferramenta de segurança, mais fácil será a tarefa de implantação da mesma no ambiente e menos conflitos causará durante e após a sua implantação.

A avaliação da ferramenta de segurança depende diretamente do ambiente global a ser protegido. Desta forma, faz-se necessário elaborar um inventário dos recursos existentes e de seus usuários, levantamento este que irá possibilitar a listagem dos aspectos relacionados com o perfil de acesso e demais características do ambiente, que deverão ser cobertos pela ferramenta de segurança.

Entretanto, deve-se ressaltar que as ferramentas de segurança, mesmo que funcionalmente semelhantes, funcionam de forma sensivelmente diferente entre si, justificando dessa forma um trabalho cuidadoso de avaliação. Mesmo a ferramenta de segurança que melhor se adapte ao ambiente para o qual foi escolhida deixará lacunas que devem ser levadas em conta na avaliação e que, em caso de escolha, devem ser preenchidas por ferramentas ou procedimentos desenvolvidos internamente ou adquiridos de outros fornecedores (CARUSO; STEFFEN, 1999).

Segundo Caruso e Steffen (1999, p. 136), nos grandes ambientes de informações, baseados em computadores de grande porte, a segurança é costumeiramente atendida por um pacote específico para controle de segurança, que, normalmente, tem interligação com a maioria dos demais pacotes usados nesse ambiente.

Após o levantamento do ambiente, pode-se montar uma planilha de avaliação específica para este ambiente, que deve constar os quesitos que a ferramenta deverá possuir para atender a situações específicas existentes em cada um dos ambientes a proteger, e que ainda poderá servir de base para se efetuar o levantamento do ambiente desejado.

A segunda etapa, de acordo com Caruso e Steffen (1999, p. 137), é a atribuição de um peso para cada item do conjunto de quesitos de avaliação, tendo como base a importância de cada quesito dentro do ambiente de informações. Os critérios de importância atribuídos a cada quesito de avaliação podem ser, por exemplo, a quantidade de pessoas que façam uso de um dado monitor de acesso e a necessidade de se manter a transparência desse processo. Ainda dentro da segunda etapa, deve-se desenvolver um sistema de pontuação para cada quesito, em função do grau de atendimento dado a esses quesitos pelo pacote avaliado.

A terceira etapa do processo consiste na avaliação propriamente dita. Segundo Caruso e Steffen (1999, p. 137), com base no levantamento efetuado, deve-se fazer a verificação da forma como cada *software* atende a cada um dos quesitos listados. Cada elemento da equipe do projeto de segurança deve fazer uma avaliação individual em relação aos outros elementos da equipe, para não haver interferência de fatores de preferência pessoal, de natureza técnica ou psicológica, sobre a avaliação; entretanto, cada elemento da equipe pode solicitar a colaboração de outros de sua própria área, tendo em vista a necessidade de levar em conta todos os aspectos possíveis relacionados com cada quesito.

Ainda de acordo com Caruso e Steffen (1999, p. 137), deve ser dada atenção especial quanto ao atendimento de quesitos dependentes de versões ou características do ambiente operacional, como, por exemplo, o fato de a proteção de programas em alguns ambientes só poder ser feita usando-se sistemas operacionais específicos com modelos específicos de equipamentos.

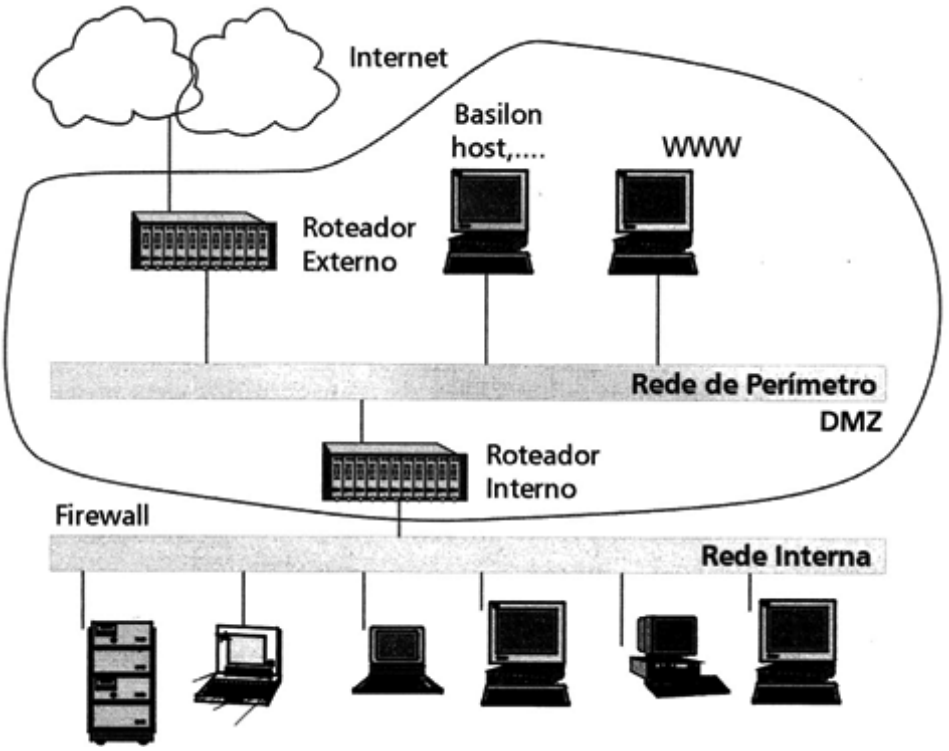
2.6 DEFINIÇÃO DE PERÍMETROS LÓGICOS

Assim como na segurança física, segundo Beal (2008, p. 95), a segurança lógica também se beneficia de barreiras criadas em torno de um ativo ou conjunto de ativos de informação que se deseja proteger. Uma defesa de perímetro é sempre um bom primeiro passo na proteção, e *firewalls* de rede, mecanismos de controle de acesso, dispositivos confiáveis de autenticação, VPNs (redes privativas virtuais construídas sobre a infraestrutura de uma rede pública, geralmente a Internet), antivírus e *bastion hosts* (*gateways* instalados entre uma rede interna e o ambiente externo para protegê-la de ataques) são exemplos de barreiras que podem ser usadas no estabelecimento de um perímetro de segurança de rede.

Um perímetro sólido de segurança lógica é difícil de implantar, em função do desafio de se identificar todas as possíveis vulnerabilidades que poderiam deixar a rede aberta a um ataque. As chamadas *redes de perímetro*, ou *zonas desmilitarizadas* (DMZ, de *de-militarized zone*) permitem proteger um computador ou segmento

de rede que fica entre uma rede interna (ex.: LAN privativa) de uma rede não confiável externa, como a internet. A DMZ atua como intermediária tanto para o tráfego de entrada quanto de saída. O termo vem do uso militar, significando uma área neutra que separa dois inimigos (BEAL, 2008).

FIGURA 13 – EXEMPLO DE REDE DE PERÍMETRO SEPARANDO A REDE INTERNA DA INTERNET



FONTE: Beal (2008, p. 96)

2.7 COMUNICAÇÃO DE DADOS E CRIPTOGRAFIA

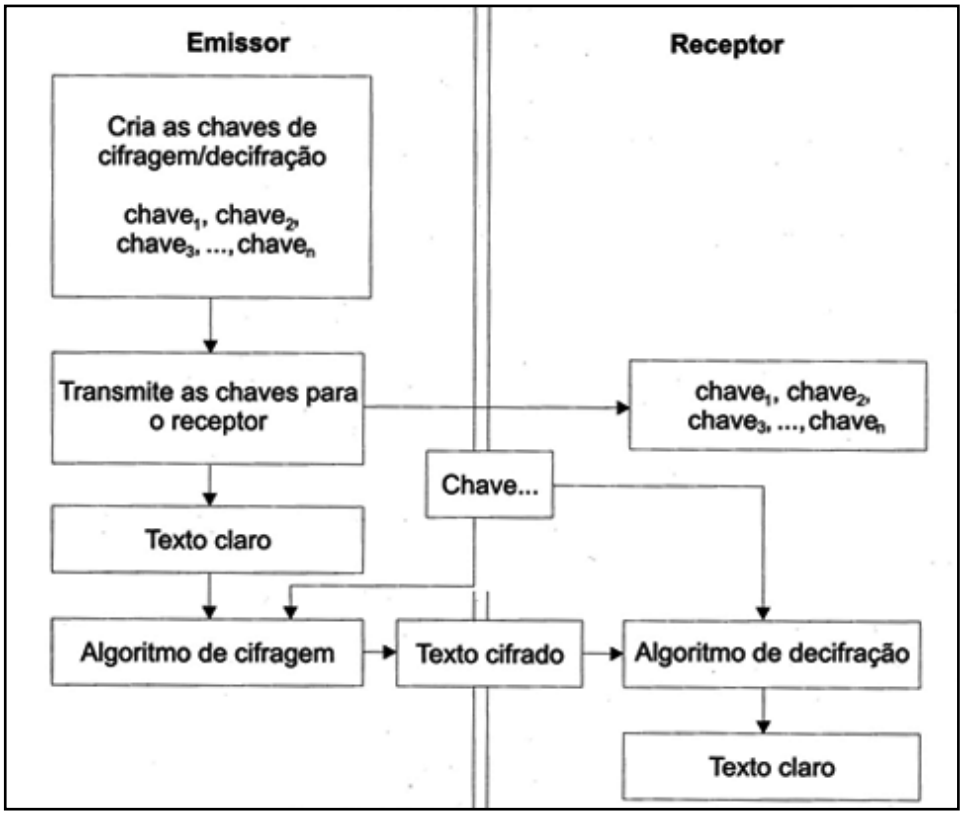
De acordo com Caruso e Steffen (1999, p. 151), um sistema de comunicação de dados é uma combinação entre *hardware*, *software*, meios de comunicação, processos e pessoas, e que no todo constitui um ambiente operacional, sendo este a principal porta de entrada para que usuários acessem o ambiente de informações e também para ataques direcionados contra este ambiente, atualmente representando um dos maiores fatores de risco.

Além dos riscos relacionados com o acesso não autorizado, segundo Caruso e Steffen (1999, p. 151), "o ambiente de comunicação de dados é também a parte mais frágil do ambiente de informações. Grande parte dos equipamentos e linhas de comunicação está fora do controle das organizações, sendo as linhas de comunicação o alvo mais frequente dos ataques ao ambiente de informações".

A internet e suas congêneres dentro das organizações, as intranets, são a vedete do momento, conforme Caruso e Steffen (1999). Os autores citam ainda que mesmo usando a criptografia para a transmissão de dados, há grande probabilidade de que algum atacante consiga desencriptar o código e fazer uso das informações; além da grande velocidade dos equipamentos, há também a grande quantidade de *hackers*, cujo único passatempo é invadir sistemas. Dada a grande quantidade de *hackers* ao redor do mundo e em razão de que, dentro da internet, tanto faz estar na sala ao lado como na China, é alta a probabilidade estatística de algum deles conseguir decodificar sua mensagem. Como qualquer outra atividade, a comunicação de dados também corre diversos riscos relacionados com o ambiente em si ou com fatores externos a ele, como ataques de invasores.

Segundo Caruso e Steffen (1999, p. 155), a criptografia é baseada sempre em um mecanismo de conversão (o algoritmo de cifragem) que converte informações de texto claro para texto cifrado usando uma chave de cifragem conhecida somente pelo emitente e do receptor (em princípio). O mecanismo pode ser de conhecimento público ou até mesmo não ser conhecido por ninguém, mas as chaves usadas no processo nunca podem ser reveladas. Devido ao risco de decifração do texto e consequente dedução da chave, estas devem ser trocadas com frequência, o que implica a possibilidade de interceptação do meio usado para comunicar as chaves entre as partes.

FIGURA 14 – ETAPAS ENVOLVIDAS NO PROCESSO DE CIFRAGEM /DECIFRAÇÃO DE MENSAGENS



FONTE: Caruso e Steffen (1999, p. 156)

A criptografia exige uma série de procedimentos de segurança, a maioria dos quais de caráter administrativo. Ela é conhecida desde a mais remota antiguidade, quando era usada principalmente para comunicações militares. Porém, foi somente neste século que o seu uso em transações comerciais tornou-se mais amplo. A criptografia pode ser usada em comunicação de dados para proteger dados sensíveis contra revelação, principalmente as transações de transferência de fundos entre bancos (CARUSO; STEFFEN, 1999).

2.8 SEGURANÇA PARA MICROS, TERMINAIS E ESTAÇÕES

Via de regra, segundo Caruso e Steffen (1999, p. 167),

> tanto os equipamentos periféricos quanto os terminais de *mainframes*, estações de trabalho e *notebooks* precisam da mesma proteção que os servidores em si, principalmente agora que desapareceram muitas das fronteiras entre equipamentos de pequeno e grande porte e que muitos microcomputadores apresentam desempenho equivalente a grandes computadores de poucos anos atrás.

Além disso, conforme Caruso e Steffen (1999, p. 167),

> a interligação cada vez maior dos computadores entre si por meio de redes de acesso públicas aumenta a vulnerabilidade dos mesmos a ataques externos. Não importa se a grande maioria dos atacantes não tenha em si propósitos criminosos; sempre haverá os que se aproveitam do conhecimento de terceiros para usos criminosos.

De acordo com Caruso e Steffen (1999, p. 168), "os equipamentos de microcomputação, terminais e estações de trabalho são menos exigentes em termos de condições ambientais que os grandes computadores". Entretanto, isso nem sempre é verdade, e não impede que os mesmos recebam tratamento de segurança similar ao dado a grandes computadores e seus periféricos. O grau de proteção dependerá somente da importância que esses equipamentos tiverem para o desenvolvimento dos negócios da organização e não somente do porte e complexidade dos equipamentos.

"Há muito tempo os computadores de pequeno porte deixaram de ser equipamentos secundários", de acordo com Caruso e Steffen (1999, p. 170). Muitos deles abrigam aplicativos importantes para as organizações que os possuem. Portanto, valem aqui as mesmas considerações feitas para equipamentos de grande porte.

Devem ser extraídas cópias de segurança (*backups*) periódicas de todos os trabalhos desenvolvidos em microcomputador, tais como: tabelas, relatórios estatísticos, planilhas etc. Essa providência facilita a recuperação das informações, precavendo-se de algum dano ou sinistro nos arquivos originais (disquetes ou

discos rígidos). Dependendo do grau de criticidade do arquivo, é aconselhável tirar mais de uma cópia de segurança. Além disso, a rotina de cópia de segurança deve emitir um histórico do processo, indicando a data, o horário, a pessoa responsável e os nomes de diretórios e arquivos envolvidos (CARUSO; STEFFEN, 1999).

Todas as cópias de segurança devem, segundo Caruso e Steffen (1999), ser guardadas em local seguro, diferente e distante dos originais. Sempre que for possível, é altamente recomendável que esse local seja em outro prédio.

2.9 SEGURANÇA EM REDES

De acordo com Caruso e Steffen (1999, p. 175), há tempos que as redes adquiriram tal grau de importância e poder de processamento que acabaram por se igualar aos grandes computadores; muitas redes têm um grau de complexidade e poder de processamento até mesmo maiores que muitos *mainframes*.

Só há uma rede imune a ataques externos: a que não tem conexão com o mundo exterior. Aliás, esse tipo de rede existe: são as redes que controlam os sistemas de armas nucleares das grandes potências militares; os computadores que controlam esse tipo de rede fazem uso de sistemas operacionais exclusivos, rodam *softwares* que somente uns poucos profissionais conhecem e todos os funcionários que trabalham com esses equipamentos são vigiados 24 horas por dia. Aquelas histórias de *hackers* que entram em computadores do Departamento de Defesa ou da NASA precisam ser mais bem explicada: eles entram em redes abertas ao público e nenhuma delas era realmente de segurança; entretanto, isso não quer dizer que esses ataques não devam ser levados a sério, principalmente com a Rússia passando por uma séria crise (CARUSO; STEFFEN, 1999).

Não há como garantir segurança absoluta em qualquer tipo de rede com acesso ao público, segundo Caruso e Steffen (1999), principalmente se estiver conectada à internet. Na realidade, não há como garantir segurança absoluta nem em redes fechadas; seres humanos são sempre muito humanos. Sempre haverá alguém que terá capacidade técnica e tempo suficiente para quebrar a segurança de sua rede; e sempre haverá alguém que não terá nenhum escrúpulo em obter lucros com as informações que ela ou alguma outra pessoa descobrir.

Conforme Caruso e Steffen (1999, p. 183), "há que se diferenciar as redes em dois tipos, em termos de acesso ao público em geral: as redes internas, de acesso restrito a funcionários da organização ou terceiros que trabalham em conjunto com a organização, e as redes externas ou públicas, abertas a todos".

A filosofia básica dos autores em relação à segurança em redes é a do "menor privilégio possível", ou seja, *o que não é explicitamente permitido, é proibido*. Essa abordagem não tornará o administrador de segurança muito popular na comunidade de usuários, mas é a mais sensata em termos de segurança; além disso, facilita a padronização e, com ela, a simplicidade. A abordagem oposta aumenta

muito a complexidade e o trabalho do administrador de segurança. As coisas mais simples são muito mais fáceis de ser entendidas; já as coisas complexas tendem a ser de entendimento mais lento e, normalmente, têm maior quantidade de "furos" e erros que comprometem a segurança (CARUSO; STEFFEN, 1999).

3 SEGURANÇA FÍSICA

Ferreira e Araújo (2008, p. 123) citam que "a segurança física desempenha um papel tão importante quanto à segurança lógica, porque é a base para a proteção de qualquer investimento feito por uma organização. Investir em diferentes aspectos da segurança sem observar suas devidas prioridades pode ocasionar uma perda de todos os recursos investidos em virtude de uma falha nos sistemas mais vulneráveis".

3.1 ASPECTOS GERAIS DA SEGURANÇA FÍSICA

De acordo com Ferreira e Araújo (2008, p. 123), "qualquer acesso às dependências da organização, desde as áreas de trabalho até aquelas consideradas severas (onde ocorre o processamento das informações críticas e confidenciais) deve ser controlado sempre fazendo necessária sua formalização".

"Os sistemas de segurança devem ser implementados para garantir que em todos os locais da organização o acesso seja realizado apenas por profissionais autorizados. Quanto maior for a sensibilidade do local, maiores serão os investimentos em recursos de segurança para serem capazes de impedir o acesso não autorizado". (FERREIRA; ARAÚJO, 2008, p. 123).

Fontes (2006, p. 126) cita três itens referentes ao acesso físico:

1) As áreas e os ambientes físicos da organização devem ter acesso restrito para visitantes e outras pessoas que não trabalham no local no dia a dia.
2) Os visitantes devem estar sempre acompanhados de alguém da organização.
3) Todas as pessoas no ambiente da organização devem estar identificadas com crachás, e qualquer colaborador deve poder questionar pessoas sem identificação.

Beal (2008) cita que um grupo específico de medidas preventivas é chamado de barreiras de segurança. Uma barreira corresponde a qualquer obstáculo colocado para prevenir um ataque, podendo ser física (cerca elétrica, parede), lógica (processo de *logon* para acesso a uma rede) ou uma combinação de ambas (autenticação de indivíduos por dispositivo biométrico para concessão de acesso, catraca eletrônica, porta aberta por cartão magnético).

A ISO 17799 (a ser detalhada na Unidade 3) utiliza a expressão *perímetro de segurança*, definindo-a como "quaisquer elementos que estabeleçam uma barreira ao acesso indevido". Uma melhor definição para perímetro de segurança seria o contorno ou linha delimitadora de uma área ou região separada de outros espaços físicos ou lógicos por um conjunto qualquer de barreiras.

Exemplos de barreiras que podem ajudar a formar um perímetro de segurança incluem salas-cofre, roletas de controle de acesso físico e uso de *token* ou dispositivo biométrico para autenticação de pessoas antes da liberação da passagem. Medidas detectivas de invasão de um perímetro de segurança podem incluir circuitos internos de TV, alarmes e sirenes e detectores de incêndio; entre outras medidas preventivas ou redutoras do impacto disponíveis estão os climatizadores de ambiente, detectores de fumaça e acionadores de água para combate a incêndio (BEAL, 2008).

"Todos os locais físicos em que se encontram recursos de informação devem possuir proteção de controle de acesso". (FONTES, 2006, p. 124).

3.2 SITUAÇÕES COMUNS DA SEGURANÇA FÍSICA

De acordo com Foina (2009, p. 179-180), os problemas mais comuns relacionados com a segurança física são:

- Roubo de insumos (tais como fitas, disquetes etc.) e de partes de microcomputadores (memórias, discos etc.).
- Acesso de pessoas não autorizadas aos relatórios com dados estratégicos da empresa, ainda que dentro do setor de Tecnologia da Informação.
- Roubo de dados armazenados em arquivos magnéticos (fitas, disquetes etc.) ou ópticos (CD-ROM, CR-RW etc.) com conteúdo de interesse da empresa (lista de clientes, arquivos de senhas etc.).
- Sabotagem em equipamentos e arquivos de dados.

A forma de minimizar tais problemas é o rígido controle de acesso às áreas sensíveis da empresa. A adoção de cartões magnéticos e bloqueios de portas tem-se mostrado eficiente contra acesso não autorizado. Certas áreas devem ter seus acessos limitados até mesmo para a maioria dos profissionais do setor (por exemplo, a fitoteca de segurança e o próprio centro de processamento). Dispositivos de identificação biométrica já estão disponíveis e devem ser usados para controlar o acesso às áreas mais críticas (FOINA, 2009).

3.3 RECOMENDAÇÕES SOBRE PROJETOS

De acordo com Caruso e Steffen (1999), um ambiente de processamento de informações, como qualquer outra instalação sensível, deve ser localizado em uma área livre de quaisquer fatores de risco, exceto se a atividade da organização, por si só, envolver esses fatores. Nesse caso, se o ambiente de processamento de informações tiver que compartilhar a área com qualquer atividade de risco, as diretrizes de segurança devem ser aplicadas de maneira ainda mais estrita.

"O mais recomendável é a construção de um edifício exclusivo, localizado no centro de uma área exclusiva, acima do nível do solo, com as instalações sensíveis no centro do edifício e as áreas de apoio na periferia, seguindo o conceito das camadas concêntricas de segurança". (CARUSO; STEFFEN, 1999, p. 210).

"A edificação deve ter toda a infraestrutura necessária pensada para permitir seu adequado funcionamento e expansão futura". (CARUSO; STEFFEN, 1999, p. 217).

Além disso, conforme Caruso e Steffen (1999), algumas atividades dentro de recintos de processamento de informações implicam riscos maiores que as demais, a exemplo dos equipamentos de impressão a *laser*, que trabalham com aquecimento e emanam gases. Sempre que for o caso, deve ser previsto um recinto separado, provido de equipamentos e dispositivos de proteção adequados para esse tipo de equipamento, se possível em outra edificação.

Caruso e Steffen (1999) comentam ainda que o funcionamento sem problemas das instalações do ambiente de informações é altamente dependente das condições que o local escolhido oferece. A escolha de um local provido de adequada infraestrutura pública reduz muito o custo final das instalações, tanto dos investimentos necessários como de manutenção no dia-a-dia.

"Uma edificação desse tipo será usada para abrigar o ambiente de informações por muitos anos, ou talvez por décadas. Desse modo, é conveniente

pensar nos detalhes que irão fazer a diferença em relação a um ambiente de trabalho de qualidade e seguro, em termos tanto de materiais empregados como de acabamento". (CARUSO; STEFFEN, 1999, p. 212).

Mesmo com os atuais equipamentos de processamento de informações tendendo a se tornar cada vez menores, segundo Caruso e Steffen (1999, p. 212-213), "instalações mais complexas, como grandes computadores e servidores de redes, precisam que as interligações entre as máquinas sejam feitas por baixo do piso".

Na medida do possível, conforme Caruso e Steffen (1999, p. 213),

> devem ser evitados tetos rebaixados, dando-se preferência a dutos aparentes, como, por exemplo, de retorno de ar-condicionado, eletrocalhas para lançamento dos cabos de energia elétrica, lógica e comunicação, instalação de luminárias, instalações de detecção e/ou extinção de incêndio.

De acordo com Caruso e Steffen (1999, p. 216), "devemos ainda observar que grandes CPDs podem funcionar sem operadores e, portanto, no escuro. Nesses casos, durante a operação normal deve-se manter a iluminação no mínimo possível, somente aumentando sua intensidade quando necessário".

"Um CPD, como qualquer outro local sensível, é uma instalação que deve ter assegurado o mais alto grau de segurança. A programação visual é parte importante do projeto porque atualmente não se considera mais tal tipo de instalação como a "vitrine" da organização". (CARUSO; STEFFEN, 1999, p. 217).

"As empresas crescem e, como consequência, a estrutura de seus ambientes de informações também precisam se expandir". (CARUSO; STEFFEN, 1999, p. 217).

3.4 PROCEDIMENTOS OPERACIONAIS

Assim que uma edificação ou qualquer outro local em que se exerça algum tipo de atividade tenha sido construído, sua infraestrutura técnica instalada e testada e tudo esteja funcionando, rapidamente se instala uma rotina diária de atividades, conforme Caruso e Steffen (1999). Esse tipo de rotina é necessário, mas ao mesmo tempo representa um risco para qualquer ramo de atividade.

Na realidade, o principal esforço administrativo dentro de qualquer organização é o estabelecimento de padrões de execução de atividades e de

comportamento de seres humanos, isto é, a rotina. Quaisquer políticas, normas e diretrizes implicam necessariamente o estabelecimento de padrões rotineiros que devem ser seguidos por todos. Ao mesmo tempo, a rotina determina um padrão estabelecido, autorizado, e qualquer desvio desse padrão implica uma possível violação de segurança (CARUSO; STEFFEN, 1999).

De acordo com Caruso e Steffen (1999, p. 259), a segurança de qualquer organização acarreta procedimentos operacionais padronizados para as inúmeras atividades exercidas dentro da mesma. Em um ambiente de informações, é necessário estabelecer padrões de procedimentos de segurança para as seguintes áreas:

- Controle de acesso;
- Prevenção e combate a incêndios;
- Controle do fornecimento de energia;
- Controle das condições ambientais;
- Entrada e saída de equipamentos, materiais e produtos;
- Segurança dos meios de armazenamento.

3.5 SEGURANÇA NOS MEIOS DE ARMAZENAMENTO

Assim como os documentos em papel, as mídias de computador (CDs, disquetes, DVDs, fitas magnéticas, discos removíveis etc.) precisam ser controladas e fisicamente protegidas, conforme Beal (2008). Além disso, ainda segundo Beal (2008, p. 84), "as mídias levadas para fora das instalações devem sujeitar-se a procedimentos de proteção e normas para que não permaneçam desprotegidas em áreas públicas".

De acordo com Caruso e Steffen (1999, p. 275), "as mídias magnéticas são muito suscetíveis às condições ambientais, principalmente ao calor e à poluição; já a tecnologia de disco óptico é bem menos sensível. Os meios de armazenamento estão sujeitos a uma série de agentes de risco, que podem afetar o conteúdo dos mesmos".

Tanto a mídia magnética como os próprios circuitos eletrônicos dos computadores são altamente suscetíveis aos efeitos dos campos magnéticos. Todavia, estes decaem muito rapidamente à medida que se afastam da fonte geradora; esse decréscimo ocorre em função do quadrado da distância da fonte emissora, e por isso é preciso uma corrente muito elevada para gerar campos suficientemente fortes (CARUSO; STEFFEN, 1999).

Segundo Caruso e Steffen (1999, p. 276-277), "campos magnéticos de 4.000A/m são fatais para mídias magnéticas. Entretanto, a 10 mm de distância é necessária uma corrente de 250 A para atingir esse valor". Mesmo assim se recomenda distâncias de segurança bem maiores, já que raios e outros transientes

podem causar picos muito altos com efeitos graves, apesar da duração de milionésimos de segundo. Emissoras de ondas de rádio e principalmente de radar merecem cuidados especiais, mesmo a distâncias variando entre 1 e 2 km.

Os filmes plásticos usados nas mídias magnéticas são suscetíveis de decomposição química em função direta do aumento da temperatura do ambiente e dos poluentes presentes na atmosfera, segundo Caruso e Steffen (1999). Além disso, os meios de armazenamento devem ser protegidos contra qualquer tipo de choque mecânico. Mesmo que, aparentemente, nada tenha sido danificado, é possível que pequenos danos comprometam a longo prazo a qualidade da mídia.

De acordo com Caruso e Steffen (1999, p. 277), "os equipamentos de armazenamento devem ser tratados até com mais cuidado que a mídia propriamente dita. Equipamentos eletrônicos, tais como CPUs, unidades de disco, memórias, unidades de comunicação etc., são tão sensíveis quanto às mídias magnéticas".

Para as mídias ópticas, conforme Caruso e Steffen (1999), recomendam-se os mesmos cuidados que para discos magnéticos rígidos, exceto com relação a campos magnéticos. Entretanto, está havendo consenso no sentido de que mídias ópticas contendo material plástico como substrato têm um limite previsto de dez anos; alguns discos ópticos especiais, que usam o vidro como substrato e o ouro como metal de revestimento e reflexão, têm tempo de vida útil previsto de 100 anos.

4 SEGURANÇA AMBIENTAL

De acordo com Beal (2008, p. 81), "a adequada proteção do ambiente e dos ativos físicos de informação, tanto como no caso do ambiente lógico, exige a combinação de medidas preventivas, detectivas e reativas".

"As proibições de fumar, tomar café, fazer refeições e outras regras de comportamento são óbvias, mas devem ser rigorosamente implementadas em todo lugar onde existir mídia magnética. Por exemplo, arquivo não é lugar de trabalho permanente, principalmente a fitoteca. É conveniente prever um ambiente para servir de copa ou local de descanso, e um local para fumantes, principalmente para o período da noite e finais de semana". (CARUSO; STEFFEN, 1999, p. 279).

De acordo com Foina (2009, p. 184), "a área de Tecnologia de Informação mantém sob sua guarda um considerável parque de equipamentos e sistemas. São equipamentos de alto valor e sensíveis a maus tratos e alterações ambientais. A fim de preservar o funcionamento desses equipamentos e a própria operação da empresa, cabe projetar a instalação adequada para suportar esse patrimônio".

Ainda de acordo com Foina (2009, p. 184),

> os cuidados a serem observados no projeto de uma instalação para Tecnologia de Informação são de ordem elétrica, ambiental (temperatura e umidade), segurança (física e patrimonial) e ergonômica. Portanto, é fundamental a organização desses recursos, para garantia da disponibilidade dos equipamentos, da segurança física e lógica, e da ergonomia dos equipamentos (facilidade de uso e garantia de boas condições de trabalho).

4.1 REDE ELÉTRICA

De acordo com Caruso e Steffen (1999, p. 284), "o prédio deve ter para-raios do tipo gaiola de Faraday, ligado a um aterramento adequado". Lembramos que o aterramento dos para-raios não pode, em hipótese alguma, estar ligado ao aterramento elétrico normal do prédio; além disso, os cabos de para-raios devem ficar o mais afastado possível de quaisquer outros cabos – elétricos, de comunicação, lógica etc. – como forma de se evitar que os mesmos sejam submetidos aos fortes campos magnéticos gerados pela passagem de descargas de relâmpagos.

Ainda segundo Caruso e Steffen (1999), os cabos de energia de grande potência, bem como os condutores de para-raios, devem ser afastados da parede externa de uma sala de segurança. A distância mínima de para-raios é de 1,0 m.

As estruturas metálicas (por exemplo, piso elevado) de uma sala devem ser ligadas ao referencial "terra" da área externa, que é ligada ao aterramento geral. Além disso, é recomendável que se interliguem todas as redes de terra que deem suporte a estações de trabalho e demais equipamentos sensíveis que estejam ligados em rede; isso permite equalizar todas as cargas entre si (CARUSO; STEFFEN, 1999).

De acordo com Caruso e Steffen (1999, p. 284), "as salas devem ter iluminação de emergência, sinalização fosforescente e farolete a pilha". Recomendamos o uso de sistemas de iluminação de emergência dotados de baterias recarregáveis. Devido ao risco de vazamento do conteúdo das pilhas comuns, recomendamos o uso de pilhas secas em faroletes.

Ainda segundo Caruso e Steffen (1999, p. 284), a luminária fluorescente deve ter reator com proteção contra superaquecimento e capacitor de segurança. Outras instalações indispensáveis devem ser do mais alto padrão de qualidade. Por fim, a energia deve ser desligada sempre que não haja equipamentos em operação dentro da sala nem pessoas trabalhando.

Ferreira e Araújo (2008, p. 125) citam cinco itens que devem ser considerados:

- A rede elétrica deve ser sempre estabilizada e dimensionada por profissionais especializados, sendo em seu planejamento, considerada a carga necessária.
- A manutenção deve ser tratada em procedimentos específicos, considerando a segurança contra incêndios.
- A fiação para o CPD deve ser única e independente para evitar a penetração de ruídos.
- Para cada ativo considerado crítico, principalmente os de processamento de dados, deve haver fornecimento de energia de forma alternativa, independente das concessionárias de energia.
- Para as situações de contingência deve-se fazer o uso de geradores de energia.

Foina (2009, p. 187) cita que boa parte dos defeitos dos computadores e periféricos ocorre em virtude de problemas de origem elétrica e de temperatura. As instalações elétricas, mesmo quando bem executadas, devem ser periodicamente revisadas para detecção de curtos-circuitos, fugas elétricas, ruptura de isolamentos, contatos oxidados, aterramento flutuante, conectores frouxos etc.

4.2 ENERGIA ALTERNATIVA

De acordo com Caruso e Steffen (1999), constatou-se uma maior preocupação com relação a sistemas *no-breaks* e geradores. Geralmente, as instalações de médio e grande porte que possuíam um grande número de aplicações *on-line* possuíam sistemas alternativos eficientes. Em alguns casos havia riscos ligados ao equipamento ou aos tanques de combustível (perigosamente próximos ao prédio).

Uma organização não funciona sem um adequado fornecimento de energia elétrica. Todos os equipamentos, independente do grau de importância, funcionam com eletricidade, das lâmpadas aos próprios computadores. Assim, é importante que seja assegurado um fornecimento constante e contínuo de energia elétrica, à prova de falhas; já na fase de projeto devem ser previstos os locais e espaço suficiente para abrigar os equipamentos de geração e condicionamento de energia elétrica (CARUSO; STEFFEN, 1999).

Caso o local escolhido sofra com problemas de falta de energia elétrica, conforme Caruso e Steffen (1999, p. 218), é recomendável prever entradas para uma fonte alternativa, capaz de abrigar as instalações destinadas à energia elétrica. Deve haver espaço para os equipamentos listados a seguir. A área total irá depender das necessidades totais de energia e da qualidade da energia fornecida:

- Transformadores.
- Estabilizadores.
- Sistema *short break*.
- Sistema motor/alternador – síncrono.
- Sistema elétrico ininterrupto de corrente alternada.
- Um grupo gerador diesel.

Dependendo da qualidade da energia elétrica disponível no local e do nível de segurança requerido pelas instalações, segundo Caruso e Steffen (1999, p. 219), é indispensável a previsão, ainda na fase de projeto, de uma série de providências para garantir o adequado fornecimento de energia. Entre elas estão:

- Espaço para condicionadores de energia.
- Locais para passagem de dutos e calhas para os cabos.
- Local para instalações de controle.
- Localização dos quadros de interligação.
- Localização dos quadros de chaves e controles da iluminação e dos equipamentos.

4.3 LOCALIZAÇÃO

A escolha da localização correta é, provavelmente, a medida isolada mais importante que se pode tomar na fase de projeto. Na medida do possível, as áreas de processamento de informações devem ser isoladas das destinadas a outras atividades por distâncias e construções corta-fogo, de acordo com a carga de incêndio existente. O simples afastamento entre dois edifícios vizinhos, cuja distância mínima é determinada pelas normas municipais, nem sempre é suficiente para proteger os equipamentos de informática de um incêndio no prédio contíguo; em princípio, uma edificação destinada a abrigar um ambiente de informações deve estar separada de qualquer outra edificação por uma distância mínima igual a, pelo menos, a altura da maior das duas edificações, mais uma folga de no mínimo 20% (CARUSO; STEFFEN, 1999).

Conforme Caruso e Steffen (1999, p. 203), "grande parte das instalações foi adaptada em prédios já existentes, nos quais não houve a preocupação com a segurança das instalações. Muitos deles estavam localizados no interior de áreas industriais de alto risco (próximos a instalações de pinturas, depósitos de inflamáveis etc.)". Durante muitos anos, o CPD de uma multinacional da Grande São Paulo funcionou dentro de um prédio de produção, junto a uma linha de pintura e em cima de depósitos de materiais inflamáveis. Detalhe: o mesmo prédio tinha sido destruído por um incêndio ainda na fase final de construção, exatamente no dia previsto para a transferência do CPD para o mesmo; ou seja, a primeira lição não foi aprendida.

Segundo Caruso e Steffen (1999), em um bairro central de São Paulo, havia uma empresa que mantinha seu CPD em uma instalação praticamente no nível da rua e com paredes de vidro temperado de 10 mm de espessura. Além de completamente visível para todos que passam pela rua, no final da tarde o sol incidia diretamente sobre o equipamento e sobre os meios magnéticos.

De acordo com Caruso e Steffen (1999, p. 220), "as instalações de processamento de informações, como qualquer outra instalação sensível, devem ser alojadas em edifício isolado ou em recinto isolado do resto do edifício por paredes divisórias corta-fogo (se possível, com paredes duplas), que vão do piso à laje de cobertura, sem interrupção (salvo as aberturas destinadas a portas, janelas e passagem de dutos)".

4.4 CLIMATIZAÇÃO

Ao se fazer um projeto de uma sala destinada a abrigar equipamentos de processamento de informações ou qualquer aplicação que implique um ambiente de alta qualidade, a exemplo de salas limpas de indústrias eletrônicas e até mesmo centros cirúrgicos, é muito importante que se pense desde o início nas instalações de climatização de ambiente (CARUSO; STEFFEN, 1999).

De acordo com Ferreira e Araújo (2008, p. 126), a utilização de equipamento de ar-condicionado exige planejamento e em muitas ocasiões, a realização de obras, envolvendo especialistas de TI e engenharia. Em localidades de processamentos de dados, visando à segurança da informação armazenada preservando sua integridade, os passos a seguir são necessários para uma avaliação adequada:

- Avaliação da capacidade mínima requerida para os equipamentos que serão armazenados neste ambiente.
- Itens de segurança contra incêndios.
- Aspectos de contingência.
- Avaliação das opções de manutenção.

Caruso e Steffen (1999, p. 219) comentam que, em uma instalação para equipamentos sensíveis, é vital que o sistema de ar-condicionado seja mantido em operação permanente; portanto, deverão ser observados os pontos listados a seguir quando do projeto das dependências para um sistema de climatização. Todos eles exigem espaço na edificação:

- Exclusividade dos equipamentos.
- Redundância.
- Localização estratégica e segura das tubulações de água e esgoto.
- Previsão da utilização de sensores nos dispositivos de controle de temperatura e umidade relativa.

- Previsão de sistemas adequados e eficientes de filtragem e vedação.
- Previsão da limpeza periódica da parte interna dos dutos do ar-condicionado.
- Instalações de água gelada.

Baseado no resultado da análise dos pontos citados, e no nível de segurança requerido pelos equipamentos, o projetista irá selecionar o sistema de condicionamento de ar mais adequado.

De acordo com Caruso e Steffen (1999), pouquíssimas empresas possuíam equipamento de ar-condicionado de reserva. Isso significa que a ocorrência de um defeito grave no sistema de climatização teria o mesmo efeito que um grave defeito do *hardware*, paralisando as instalações da mesma forma. Anos atrás, o CPD de uma grande estatal paulista dividia os seus equipamentos de ar-condicionado com o auditório que ficava no andar superior. Sempre que havia algum evento no auditório, a temperatura do CPD chegava à casa dos 35º C.

Caruso e Steffen (1999, p. 219-220) citam três dicas importantes sobre a infraestrutura para climatização:
1) Na implantação de uma instalação para ambientes de informações, o sistema central de condicionamento de ar é vital ao seu pleno funcionamento.
2) Devido à necessidade do controle das condições ambientais e de confiabilidade para o sistema de condicionamento de ar, é recomendável a instalação de condicionadores do tipo compacto (*self-contained*) ou de central de água gelada.
É conveniente que a água de condensação, gerada pelo sistema de climatização, seja canalizada diretamente para um dreno capaz de suportar o volume máximo de água condensada pelo ar-condicionado, com uma folga de pelo menos 50%.

4.5 PREVENÇÃO E COMBATE A INCÊNDIO

Segundo Caruso e Steffen (1999, p. 266), "o incêndio é, provavelmente, o desastre mais temido por seres humanos". Nenhum outro tipo de desastre isolado provoca mais danos; além da destruição física dos bens que pegam fogo, há diversas outras consequências, como intoxicação e envenenamento provocados pelos gases da combustão nos seres vivos, corrosão decorrente dos gases corrosivos e tóxicos desprendidos pelas chamas e até mesmo danos nas instalações permanentes que devem ser reparados.

Não há pessoa que não conheça o fogo e seus efeitos sobre o meio ambiente, conforme Caruso e Steffen (1999, p. 266). Entretanto, somente as pessoas com treinamento voltado para prevenção e combate a incêndios recebem informações gerais a respeito.

Levando-se em conta a grande quantidade de produtos, dispositivos, mobiliários e equipamentos fabricados com materiais combustíveis que os seres humanos usam no dia a dia, é grande o risco que locais por eles ocupados frequentemente se incendeiem. Entretanto, medidas tomadas desde o início da construção das instalações podem minimizar os riscos de um eventual incêndio, e, em caso de ocorrência, tornar sua propagação mais difícil e reduzir o montante dos danos (CARUSO; STEFFEN, 1999).

As instalações de um ambiente de informações, de acordo com Caruso e Steffen (1999, p. 220), devem ser projetadas de maneira que reduzam ao mínimo o risco de fogo na edificação ou em qualquer equipamento, dispositivo ou material que sirva para gerar ou propagar fogo.

De acordo com Ferreira e Araújo (2008, p. 126), "os detectores de fumaça e temperatura devem ser instalados com a orientação de um técnico especializado e podem estar localizados, no mínimo, sob os pisos falsos e sobre os tetos suspensos".

Caruso e Steffen (1999) citam que a maioria das instalações, inclusive muitas de grande porte, não possuía equipamentos de sensoriamento e alarme contra gases e fogo, dispondo apenas do equipamento básico exigido por lei (extintores manuais). Alguns possuíam alarmes de acionamento manual (quebra de vidro), que dependem da ação humana. Vimos também instalações dotadas de hidrantes e *sprinklers*. Em si, os *sprinklers* e os hidrantes não são um problema; este reside na forma de operação do sistema de *sprinklers* e dos hidrantes.

Ferreira e Araújo (2008, p. 127) citam que os *sprinklers* de água (combate ao fogo por meio de aspersão), não devem ser instalados nos locais de processamento de dados, deve haver instalados alarmes interligados a uma central de monitoramento e segurança, além de os locais de armazenamento de mídias de *backups* devem ser realizados em cofres antichamas, trancados com senha e localizados de forma distante de onde se efetua o processamento dos dados.

Nas instalações dotadas de sensores automáticos, conforme Caruso e Steffen (1999), sua distribuição nem sempre era a mais adequada. Poucas instalações realizavam testes periódicos de funcionamento. Na maioria dos casos, a sinalização de emergência era inadequada ou incompleta e não possuía iluminação de emergência.

Conforme Ferreira e Araújo (2008, p. 126), "a utilização de sistemas de detecção de incêndio de forma automática deve ser obrigatória, de forma a acionar alarmes e recursos de combate quando identificado qualquer início de incêndio. Deve haver brigada de incêndio, constituída formalmente e treinada".

De acordo com Caruso e Steffen (1999, p. 203), "alguns gerentes tinham a ideia falsa de que havia pessoal treinado para combate a incêndios; entretanto, após entrevistas com o pessoal operacional, notava-se que a maioria tinha feito apenas um curso teórico havia tempos (nunca mais reciclado). Constatou-se que instalações com turnos de operação de madrugada não possuíam nenhum elemento treinado nesse período".

Ferreira e Araújo (2008) citam que, quanto mais críticos forem os equipamentos para o negócio, mais investimentos em recursos devem ser efetuados, com um técnico de segurança avaliando a necessidade da utilização dos seguintes recursos:
- Uso de equipamentos para extinção automática.
- Uso de portas corta-fogo.
- Uso de alarmes de incêndio e detectores de fumaça.

4.6 INSTALAÇÃO, PROTEÇÃO E MANUTENÇÃO DE EQUIPAMENTOS

De acordo com Beal (2008), a instalação de qualquer tipo de equipamento relacionado à TI deve ser precedida de uma avaliação do ambiente para reduzir o grau de exposição e acessos desnecessários, sabotagem, espionagem etc. Entre as ameaças a serem consideradas no estabelecimento de controles, estão: roubo, fogo, explosivos, fumaça, água (ou falha de abastecimento), poeira, vibração, efeitos químicos, interferência no fornecimento de energia elétrica e radiação eletromagnética.

Ainda segundo Beal (2008, p. 88), políticas específicas para a restrição de alimentos, bebidas e fumo próximo às instalações de processamento da informação, monitoração de aspectos ambientais que possam afetar essas instalações, uso de métodos de proteção como capas para teclados em ambientes industriais são controles citados pela norma ISO 17799 (a ser estudada na Unidade 3), que também

recomenda a consideração de desastres que possam ocorrer nas proximidades da instalação (prédios vizinhos, andares superiores ou inferiores etc.).

A adequada manutenção dos equipamentos é necessária para a garantia de sua integridade e disponibilidade. A ISO 17799 (item 7.2.4) recomenda a realização de manutenções de acordo com as especificações e os intervalos indicados pelo fabricante, uso de pessoal qualificado para a execução dos reparos, registro de falhas suspeitas e das manutenções corretivas e preventivas realizadas, controles apropriados para o envio de equipamentos para manutenções fora da organização (incluindo as considerações de segurança em relação a dados apagados que minimizar os riscos de vazamento de informações) (BEAL, 2008).

4.7 REMOÇÃO, DESCARTE E TRANSPORTE DE EQUIPAMENTOS

Controles específicos devem ser implementados para evitar vazamento de informações, remoção não autorizada de propriedade e furto de equipamentos ou peças e dispositivos de equipamentos retirados da organização, entre outros riscos relativos à remoção, descarte e transporte de equipamentos. Exemplos de controles aplicáveis são: verificação da eliminação segura de informações sensíveis e de *software* licenciado de discos rígidos antes de sua transferência ou descarte, inspeção de equipamentos retirados e devolvidos à organização e transporte de equipamentos portáteis em viagens sempre que possível como bagagem de mão e dentro de receptáculos que disfarcem seu conteúdo (BEAL, 2008).

4.8 PROTEÇÃO DE DOCUMENTOS EM PAPEL

De acordo com Beal (2008, p. 83), a adequada proteção dos documentos em papel implica a existência de procedimentos de tratamento que cubram no mínimo os seguintes aspectos:

- Cópia.
- Armazenamento.
- Transmissão pelo correio ou *fax*.
- Descarte seguro.

Caso a organização dependa de documentos em papel para cumprir sua missão e alcançar seus objetivos, segundo Beal (2008, p. 83), ela deve dispor pelo menos dos seguintes controles para a proteção desses ativos de informação:

- Uso de rótulos para identificar documentos que requerem tratamento confidencial.
- Política de armazenamento de papéis que assegure a guarda em local protegido (de preferência em cofre ou arquivo resistente a fogo) de papéis com informações confidenciais ou críticas para o negócio.
- Procedimentos especiais para a impressão e transmissão via *fax* de documentos confidenciais (incluindo supervisão da impressora durante o processo de impressão e proteção contra discagem incorreta ou uso de números errados guardados na memória do aparelho de *fax*).
- Recepção e envio controlado de correspondência sigilosa.

Itens sensíveis, como cheques e notas fiscais em branco, precisam estar submetidos a controles adicionais compatíveis com os níveis de risco identificados (BEAL, 2008).

4.9 PROTEÇÃO DE COMUNICAÇÕES NÃO BASEADAS EM COMPUTADOR

De acordo com Beal (2008), a troca de informação por comunicação verbal, *fax*, vídeo etc. pode ser comprometida caso inexistam políticas e procedimentos adequados à utilização desses recursos. Iremos estudar na Unidade 3 que a ISO 17799 (item 8.7.7) relaciona como problemas a serem considerados a escuta de conversas pelo uso de telefones em locais públicos ou de mensagens armazenadas em secretárias eletrônicas e sistemas de correio de voz, o envio acidental de *fax* para o número errado, a possibilidade de prejuízo às operações de negócio em caso do comprometimento dos recursos de comunicação por sobrecarga ou interrupção do serviço. Os funcionários devem ser alertados sobre as precauções a serem adotadas para evitar esses e outros problemas que possam levar à interceptação de conversas ou informações confidenciais ou à indisponibilidade do serviço quando do uso de comunicação por voz, *fax* e vídeo.

4.10 POLÍTICA DE MESA LIMPA E TELA LIMPA

Segundo Beal (2008), esta política visa reduzir os riscos de acesso não autorizado às informações corporativas, que se tornam mais vulneráveis quando papéis, mídias removíveis são deixados sobre a mesa e computadores são deixados ligados e conectados a sistemas ou redes na ausência do responsável. Entre as medidas de proteção sugeridas pela ISO 17799, a serem aplicadas fora do horário normal de trabalho (item 7.3.1), estão a guarda de mídias e papéis críticos ou sensíveis em cofre ou arquivo resistente a fogo, o desligamento de computadores e impressoras e sua proteção por senhas, chaves ou outros controles e o travamento de copiadoras (ou sua proteção contra uso não autorizado).

RESUMO DO TÓPICO 2

Caro(a) acadêmico(a)! Neste segundo tópico, você estudou os seguintes aspectos:

- Os aspectos gerais da segurança da informação no contexto lógico.
- A definição da estrutura da administração e da equipe responsável pela segurança da informação.
- O levantamento dos usuários, recursos e ferramentas que serão utilizados para garantir a segurança.
- A definição de perímetros lógicos através de equipamentos e *softwares* de segurança.
- A segurança na transmissão de dados pela internet através da tecnologia de criptografia.
- Os aspectos gerais da segurança da informação no contexto físico.
- As recomendações para a definição do espaço físico onde serão alocados os equipamentos contendo as informações.
- Os cuidados que devem ser despendidos sobre as mídias de armazenamento.
- A segurança ambiental, no que tange à rede elétrica, à energia alternativa, à climatização, entre outros fatores que devem ser levados em conta para o bom funcionamento dos equipamentos e consequentemente a segurança das informações.

AUTOATIVIDADE

1 As barreiras de segurança são obstáculos que visam garantir que um ativo ou um conjunto de ativos de informação sejam protegidos de acessos indevidos. Uma das barreiras que pode ser utilizada é o controle de acesso realizado através da utilização de dados biométricos.

( ) CERTO.
( ) ERRADO.

2 Ao selecionar um profissional para ser o Administrador de Segurança, algumas características do seu perfil deverão ser analisadas. Entre elas estão:

a) ( ) Segurança no ambiente, experiência, espírito inventivo e legitimidade emocional.
b) ( ) Conhecimento do ambiente informacional, experiência, facilidade de relacionamento e responsabilidade.
c) ( ) Controle do ambiente, liderança, estabilidade espiritual e facilidade comportamental.
d) ( ) Conhecimento dos recursos, espontaneidade, liderança e responsabilidade.

Assista ao vídeo de resolução da questão 1

TÓPICO 3

SEGURANÇA EM SISTEMAS DISTRIBUÍDOS

1 INTRODUÇÃO

Muitos recursos de informação que se tornam disponíveis e são mantidos em sistemas distribuídos têm um alto valor intrínseco para seus usuários. Portanto, sua segurança é de considerável importância (GROSS, 2008).

A segurança de recursos de informação, de acordo com Coulouris, Dollimore e Kindberg (2007), possui três componentes: integridade (proteção contra danos ou alterações), disponibilidade (proteção contra interferência com os meios de acesso aos recursos) e confidencialidade (proteção contra exposição e acesso para pessoas não autorizadas).

Segundo Gross (2008, p. 13), "mesmo que a internet permita que um programa em um computador se comunique com um programa em outro computador, independentemente de sua localização, existem riscos de segurança associados ao livre acesso a todos os recursos de uma intranet".

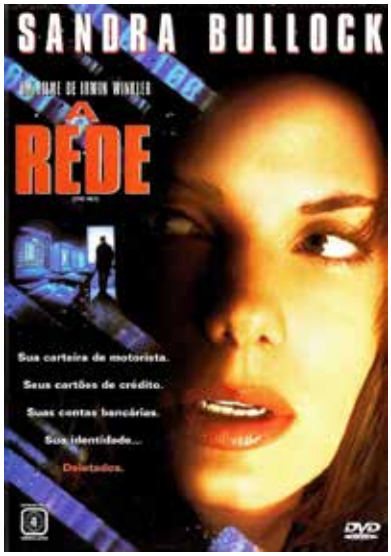
"Embora um *firewall* possa ser usado para formar uma barreira em torno de uma intranet, restringindo o tráfego que pode entrar ou sair, isso não garante o uso apropriado dos recursos pelos usuários de dentro da intranet, nem o uso apropriado de recursos na internet, que não são protegidos por *firewalls*". (GROSS, 2008, p. 13).

De acordo com a Cyclades Brasil (2001), "um *firewall* não é um equipamento ou *software*, e sim um conjunto formado por *hardware*, *software* e uma política de segurança (documentos que contém diretrizes para tomada de decisão sobre segurança na empresa). O *firewall* tem por função controlar o tráfego entre duas ou mais redes, visando fornecer segurança a uma (ou algumas) das redes que normalmente tem informações e recursos que não devem estar disponíveis aos usuários de outra(s) rede(s)".

Em um sistema distribuído, segundo Gross (2008, p. 13), os clientes enviam pedidos para acessar dados gerenciados por servidores, envolvendo o envio de informações através de mensagens por uma rede. Por exemplo:

- Um médico pode solicitar acesso aos dados de pacientes de um hospital ou enviar mais informações sobre tais pacientes.
- No comércio eletrônico e nos serviços bancários, usuários enviam números de seus cartões de crédito pela internet.

Nada melhor do que aprender algo assistindo a um bom filme. Muitos são os filmes retratando problemas de segurança na internet ou em redes de computadores. Este é muito bom! A Rede.



Ela não tem mais cartão de crédito, conta bancária, carteira de motorista,... e perdeu ainda o número da identidade. Foi tudo "deletado". Ela simplesmente deixou de existir! Sandra Bullock, Jeremy Northam e Dennis Miller estrelam este suspense sobre uma especialista em computadores cuja vida é apagada por uma conspiração eletrônica.

Angela Bennett (Sandra Bullock) é uma analista de sistemas *freelance* que passa os dias procurando por vírus de computador, e as noites 'conversando' com outros tímidos fanáticos pelo cyber-espaço na rede internet. Nessa rotina solitária ela se sente tranquila e feliz, mantida em sua redoma protetora... até que o mundo eletrônico que ela criou a faz mergulhar numa criminosa teia de corrupção e conspiração. Enquanto conserta alguns defeitos num programa de *games*, Angela acessa um quebra-cabeças com dados altamente secretos do governo. Rapidamente percebe que penetrou numa conspiração por computador, e que sinistros piratas da informática não se deterão enquanto ela não for eliminada. Angela descobre que todos os traços de sua existência foram apagados e que recebeu uma nova identidade nos arquivos da polícia e se tornara uma criminosa com a cabeça a prêmio. Agora ela vai ter que sair da frente do computador e escapar com vida no mundo real.

A REDE. Direção de Irwin Winkler. EUA: Sony Pictures Entertainment, 1995, DVD (114 min), color.

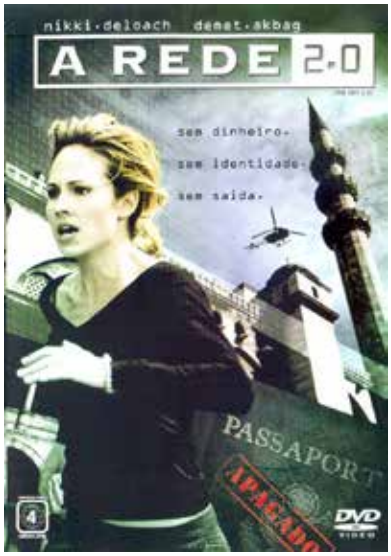
Ambos os exemplos, segundo Gross (2008, p. 14), "trazem o desafio de enviar informações sigilosas em uma ou mais mensagens, através de uma rede, de modo seguro. Mas segurança não é apenas uma questão de ofuscar o conteúdo de mensagens – ela também envolve saber com certeza a identidade do usuário, ou outro agente, em nome de quem as mensagens foram enviadas.

No primeiro exemplo, o servidor precisa saber se o usuário é realmente um médico, e no segundo exemplo o usuário precisa ter a certeza da identidade da loja ou do banco com o qual está transacionando.

O segundo desafio consiste na identificação correta de um usuário ou agente remoto. Ambos os desafios podem ser resolvidos usando técnicas de criptografia desenvolvidas para este fim, sendo amplamente usadas na internet.

Prepare a pipoca! Outro filme interessante e que traz alguns pontos importantes sobre segurança é A Rede 2.0:

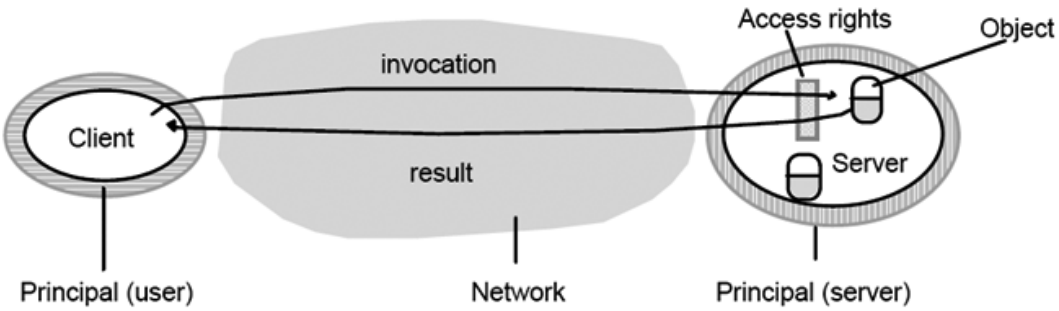
De um dos produtores do mega sucesso A Rede, esta sequência de ação é estrelada por Nikki DeLoach (da série de TV North Shore) que interpreta Hope Cassidy, uma linda especialista em computadores que viaja para Istambul em busca do trabalho perfeito, mas logo fica presa a uma enrascada de alta tecnologia. A perseguição interminável começa quando Hope tem que usar sua inteligência e beleza para recuperar seu nome e revelar o mistério. Graças à ajuda de um misterioso motorista de táxi e de uma sexy aeromoça, ela é capaz de descobrir a chocante verdade sobre o que está acontecendo com ela. Será que ela poderá recuperar seu passado antes que os bandidos apaguem seu futuro? Ou será que ela será capturada na rede?
A REDE 2.0. Direção de Mike Bigelow. EUA: Sony Pictures Entertainment, 2006, DVD (92 min), color.



2 PROTEÇÃO DE OBJETOS EM UM SISTEMA DISTRIBUÍDO

A figura a seguir ilustra um servidor gerenciando um conjunto de objetos para alguns usuários. Os usuários podem executar programas clientes que enviam requisições para o servidor a fim de realizar operações sobre este conjunto de objetos. O servidor executa a operação especificada em cada invocação e envia o resultado da execução para o cliente.

FIGURA 15 – OBJETOS E PRINCIPAIS DAS INVOCAÇÕES



FONTE: Adaptado de COULOURIS, G.; DOLLIMORE, J.; KINDBERG, **T. Distributed Systems**: Concepts and Design. 3. ed. England: Addison Wesley, 2001.

Segundo Coulouris, Dollimore e Kindberg (2007), os objetos possuem diferentes usos por diferentes usuários. Por exemplo, alguns objetos podem conter dados privativos de um usuário, como sua caixa de correio, e outros objetos podem conter dados compartilhados, como suas páginas web. Para dar suporte a isso, definem-se direitos de acesso especificando quem pode executar operações sobre um objeto – por exemplo, quem pode ler ou gravar seu estado.

Assim, usuários devem ser inclusos no modelo de segurança como beneficiários dos direitos de acesso. Isso é feito associando a cada invocação, e a cada resultado, o tipo de autorização de quem a executa. Essa autorização é chamada *principal*. Um "principal" pode ser um usuário ou um processo. Na figura acima, a invocação vem de um usuário e o resultado vem de um servidor.

De acordo com Gross (2008), a responsabilidade por verificar a identidade do "principal" que efetua cada invocação e conferir se este tem direitos de acesso para efetuar a operação solicitada no objeto, recusando as que não são permitidas, recai sobre o servidor. O cliente pode verificar a identidade do principal que está por trás do servidor, de modo a garantir que o resultado seja enviado realmente por esse servidor.

3 PROTEÇÃO DE PROCESSOS E SUAS INTERAÇÕES

De acordo com Coulouris, Dollimore e Kindberg (2007), processos interagem através do envio de mensagens, expostas a ataques, pois o acesso à rede e serviços de comunicação deve ser livre, permitindo que ambos os processos interajam entre si. Servidores e processos pares publicam suas interfaces, permitindo que sejam enviadas invocações a eles por qualquer processo.

Frequentemente, segundo Gross (2008, p. 88), "sistemas distribuídos são implantados e usados em tarefas que podem estar sujeitas a ataques externos provenientes de usuários mal-intencionados". Isso é especialmente verdade para aplicativos que efetuam transações financeiras, manipulam informações confidenciais ou secretas, ou outro tipo de informação cujo segredo ou integridade seja crucial.

De acordo com Gross (2008, p. 88), a integridade é ameaçada por violações de segurança, bem como falhas na comunicação. Sabemos que podem existir ameaças aos processos que compõem os aplicativos e às mensagens que trafegam entre eles. Porém como podemos analisar tais ameaças visando a sua identificação e anulação? A seguir é apresentado um modelo para efetuar esta análise de ameaças à segurança.

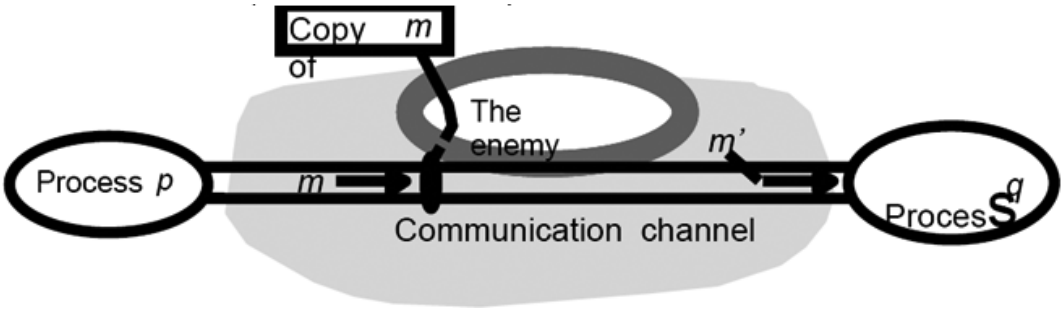
4 O INVASOR

Para modelar as ameaças à segurança, postulamos um invasor (por vezes conhecido como atacante), que é capaz de enviar qualquer mensagem para qualquer processo e ler ou copiar qualquer mensagem entre processos, como demonstra a figura a seguir.

Tais ataques podem ser realizados usando-se simplesmente um computador conectado a uma rede para executar um programa que lê as mensagens endereçadas para outros computadores da rede, ou por um programa que gere mensagens que façam falsos pedidos para serviços e deem a entender que sejam provenientes de usuários autorizados. O ataque pode vir de um computador legitimamente conectado à rede, ou de um que esteja conectado de maneira não autorizada (COULOURIS; DOLLIMORE; KINDBERG, 2007).

As ameaças de um potencial atacante serão discutidas nos próximos tópicos: ameaças aos processos, ameaças aos canais de comunicação, e outras ameaças possíveis.

FIGURA 16 – O INIMIGO (INVASOR OU ATACANTE)



FONTE: Adaptado de COULOURIS, G.; DOLLIMORE, J.; KINDBERG, **T. Distributed Systems**: Concepts and Design. 3. ed. England: Addison Wesley, 2001.

4.1 AMEAÇAS AOS PROCESSOS

De acordo com Coulouris, Dollimore e Kindberg (2007), um processo projetado para tratar pedidos pode receber uma mensagem de outro processo no sistema distribuído e não ser capaz de determinar identidade real do remetente. Protocolos de comunicação como o IP incluem o endereço do computador de origem em cada mensagem, mas não é difícil um atacante gerar uma mensagem com um endereço falso de origem. Essa falta de reconhecimento confiável da origem de mensagens é, segundo explicação a seguir, uma ameaça ao funcionamento correto tanto de servidores quanto de clientes:

- Servidores: como um servidor pode receber pedidos de uma grande diversidade de clientes, ele não pode necessariamente determinar a identidade do "principal" por trás de uma invocação em especial. Mesmo que o servidor exija a inclusão da identidade do principal em cada requisição, um atacante pode gerá-la usando uma identidade falsa. Sem reconhecimento garantido da identidade do remetente, o servidor pode não saber se deve executar a operação ou recusá-la. Por exemplo, um servidor de correio eletrônico recebe de um usuário uma solicitação de leitura de mensagens de uma caixa de correio em especial, e pode não saber se o usuário em questão pode fazer isso ou se é uma solicitação indevida.

- Clientes: quando um cliente recebe o resultado de uma requisição feita a um servidor, ele pode não identificar se a origem da mensagem com o resultado é mesmo do servidor desejado ou de um invasor fazendo *spoofing* desse servidor.

"O *spoofing* é, na prática, o roubo de identidade. Assim, um cliente poderia receber um resultado não relacionado à invocação original, como por exemplo, uma mensagem falsa de correio eletrônico (que não está na caixa de correio do usuário)". (GROSS, 2008, p. 89).

4.2 AMEAÇAS AOS CANAIS DE COMUNICAÇÃO

De acordo com Coulouris, Dollimore e Kindberg (2007), um invasor pode copiar, alterar ou inserir mensagens quando elas trafegam pela rede e em seus sistemas intermediários (por exemplo, roteadores).

Estes ataques representam uma ameaça à integridade das informações e à privacidade quando elas trafegam pela rede, além da própria integridade do

sistema. Por exemplo, uma mensagem contendo um correio eletrônico de um usuário pode ser revelada a outro, ou ser alterada para dizer algo totalmente diferente.

Outra forma de ataque é a tentativa de salvar cópias de mensagens e reproduzi-las posteriormente, tornando possível a reutilização da mesma mensagem repetidas vezes. Por exemplo, alguém pode tirar proveito, reenviando uma mensagem de invocação, solicitando uma transferência de um valor em dinheiro de uma conta bancária para outra.

De acordo com Gross (2008, p. 90), essas ameaças podem ser anuladas a partir do uso de canais seguros de comunicação, descritos a seguir e baseados em autenticação e criptografia.

5 ANULANDO AMEAÇAS À SEGURANÇA

A seguir apresentaremos as principais técnicas, conforme Coulouris, Dollimore e Kindberg (2007), nas quais os sistemas seguros são baseados.

5.1 CRIPTOGRAFIA E SEGREDOS COMPARTILHADOS

Suponha que dois processos (por exemplo, um cliente e um servidor) compartilhem um segredo; isto é, ambos conhecem o segredo, mas nenhum outro processo no sistema distribuído sabe dele. Então, se uma mensagem trocada por esses dois processos incluir informações que provem o conhecimento do segredo compartilhado por parte do remetente, o destinatário saberá com certeza que o remetente foi o outro processo do par. É claro que se deve tomar os cuidados necessários para garantir que o segredo compartilhado não seja revelado a um invasor (COULOURIS; DOLLIMORE; KINDBERG, 2007).

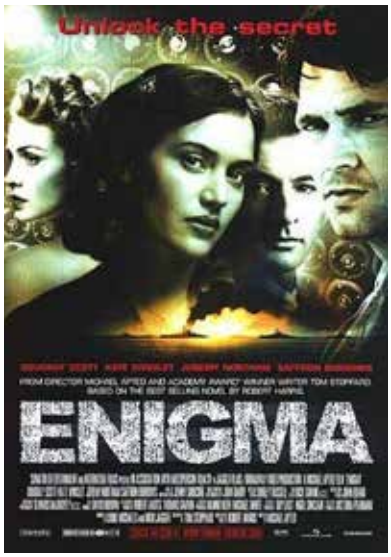
Criptografia é a ciência de manter as mensagens seguras, e cifrar é o processo de embaralhar uma mensagem de maneira a ocultar o seu conteúdo. A criptografia moderna é baseada em algoritmos que utilizam chaves secretas – números grandes e difíceis de adivinhar – para transformar os dados de uma maneira que só possam ser revertidos com o conhecimento da chave de descriptografia correspondente. (GROSS, 2008, p. 90).

DICAS

Vamos assistir a outro grande filme, que ilustra a utilização de criptografia a partir da famosa máquina Enigma, usada pelos submarinos alemães durante a segunda guerra mundial para a criptografia de mensagens?

Tom Jericho (Dougray Scott) é o matemático responsável pela descoberta do Enigma, um código secreto que os navios nazistas usavam para se comunicar durante a Segunda Guerra Mundial. Mas os nazistas alteraram o código e o Serviço Secreto Britânico chama Tom para decifrá-lo novamente. Paralelamente, sua namorada Claire (Saffron Burrows) some misteriosamente e o Serviço Secreto parece muito preocupado com isso. Desesperado, Tom procura Hester Wallace (Kate Winslet), melhor amiga de Claire, que começa a ajudá-lo. Enquanto sua equipe se empenha para descobrir a chave do novo código, Tom e Hester investigam o desaparecimento de Claire e, a cada pista, eles percebem que se trata de mais um enigma.

ENIGMA. Direção de Michael Apted. EUA: Manhattan Pictures International / Jagged Films, 2001, DVD (117 minutos), color.



5.2 AUTENTICAÇÃO

De acordo com Coulouris, Dollimore e Kindberg (2007), o uso de segredos compartilhados e da criptografia fornece a base para a autenticação de mensagens – provar as identidades de seus remetentes. A técnica de autenticação básica consiste em incluir em uma determinada mensagem uma parte cifrada que possua conteúdo suficiente para garantir a sua autenticidade.

A autenticação de uma requisição para leitura de partes de um arquivo enviado ao servidor de arquivos pode, por exemplo, incluir uma representação da identidade do "principal" fazendo a requisição, a identificação do arquivo e a data e hora da requisição, tudo cifrado utilizando uma chave secreta compartilhada entre o servidor de arquivos e o processo requisitante. O servidor decifra o pedido e verifica se de fato correspondem realmente à requisição.

5.3 CANAIS SEGUROS

Segundo Coulouris, Dollimore e Kindberg (2007), criptografia e autenticação são usadas para construir canais seguros como uma camada de serviço adicional sobre os serviços de comunicação existentes. Um canal seguro consiste de um canal de comunicação conectando dois processos, cada qual atuando em nome de um "principal", como visto na figura a seguir.

FIGURA 17 – COMUNICAÇÃO ENTRE PROCESSOS USANDO UM CANAL SEGURO

FONTE: COULOURIS, G.; DOLLIMORE, J.; KINDBERG, **T. Sistemas Distribuídos**: Conceitos e Projeto. 4. ed. Porto Alegre: Bookman, 2007.

Um canal seguro tem as seguintes propriedades:

- Cada processo conhece com certeza a identidade do "principal" em nome de quem o outro processo está executando. Portanto, se um cliente e um servidor se comunicam através de um canal seguro, o servidor conhece a identidade do principal que está por trás das invocações e verifica seus direitos de acesso antes da execução de uma operação. Isso permite ao servidor a correta proteção de seus objetos e ao cliente a certeza de que está recebendo resultados de um servidor confiável.

- Canais seguros garantem a privacidade e integridade (proteção contra falsificação) dos dados transmitidos por eles.

- Cada mensagem inclui uma indicação de relógio lógico, ou físico, impedindo que as mensagens sejam reproduzidas ou reordenadas.

De acordo com Gross (2008, p. 92), a construção e utilização de canais seguros vêm se tornado uma ferramenta prática visando proteger o comércio eletrônico e as comunicações de modo geral.

6 OUTRAS POSSÍVEIS AMEAÇAS

A seguir apresentaremos duas ameaças à segurança: ataques de negação de serviço e utilização de código móvel, consideradas possíveis oportunidades para invasores romperem as atividades dos processos.

6.1 NEGAÇÃO DE SERVIÇO

De acordo com Coulouris, Dollimore e Kindberg (2007), esta é uma forma de ataque na qual o atacante interfere nas atividades dos usuários autorizados, fazendo inúmeras invocações sem sentido em serviços ou transmitindo mensagens incessantemente em uma rede, gerando uma sobrecarga dos recursos físicos (capacidade de processamento do servidor, largura de banda da rede etc.).

Normalmente tais ataques são feitos visando retardar ou impedir as invocações válidas de outros usuários. Por exemplo, a operação de trancas eletrônicas de portas de um prédio poderia ser desativada por um ataque saturando o computador que controla as trancas com pedidos inválidos.

6.2 CÓDIGO MÓVEL

De acordo com Coulouris, Dollimore e Kindberg (2007), o código móvel levanta novos problemas de segurança para quaisquer processos que recebam e executem códigos provenientes de outro lugar. Estes códigos podem facilmente desempenhar o papel de cavalo de Troia, dando a entender que vão cumprir um propósito inocente, mas na verdade incluem códigos que acessam ou modificam recursos legitimamente disponíveis para os usuários que os executam.

Os métodos pelos quais tais ataques podem ser realizados são muitos e variados. Para evitá-los, o ambiente que recebe estes códigos deve ser construído com muito cuidado. Muitos desses problemas foram resolvidos utilizando Java e outros sistemas de código móvel, mas a história recente desse assunto traz algumas vulnerabilidades embaraçosas. Isso ilustra bem a necessidade da análise rigorosa no projeto de todos os sistemas seguros.

7 USO DOS MODELOS DE SEGURANÇA

Pode-se pensar que a obtenção de segurança em sistemas distribuídos seria uma questão simples, envolvendo o controle do acesso a objetos de acordo com direitos de acesso predefinidos e com o uso de canais seguros para comunicação. Infelizmente, geralmente esse não é o caso. O uso de técnicas de segurança como a criptografia e o controle de acesso acarreta custos de processamento e gerenciamento substanciais (COULOURIS, DOLLIMORE; KINDBERG, 2007).

O modelo de segurança delineado anteriormente fornece a base para a análise e o projeto de sistemas seguros, onde esses custos são mantidos em um mínimo. Entretanto, as ameaças a um sistema distribuído surgem em muitos pontos, e é necessária uma análise cuidadosa das ameaças que podem surgir de todas as fontes possíveis no ambiente de rede, no ambiente físico e no ambiente humano do sistema. Essa análise envolve a construção de um modelo de ameaças,

listando todas as formas de ataque às quais o sistema está exposto e uma avaliação dos riscos e consequências de cada um. A eficácia e o custo das técnicas de segurança necessárias podem então ser ponderadas em relação às ameaças (COULOURIS; DOLLIMORE; KINDBERG, 2007).

LEITURA COMPLEMENTAR

CAPITAL INTELECTUAL: NOVO ALVO DOS CRIMES VIRTUAIS

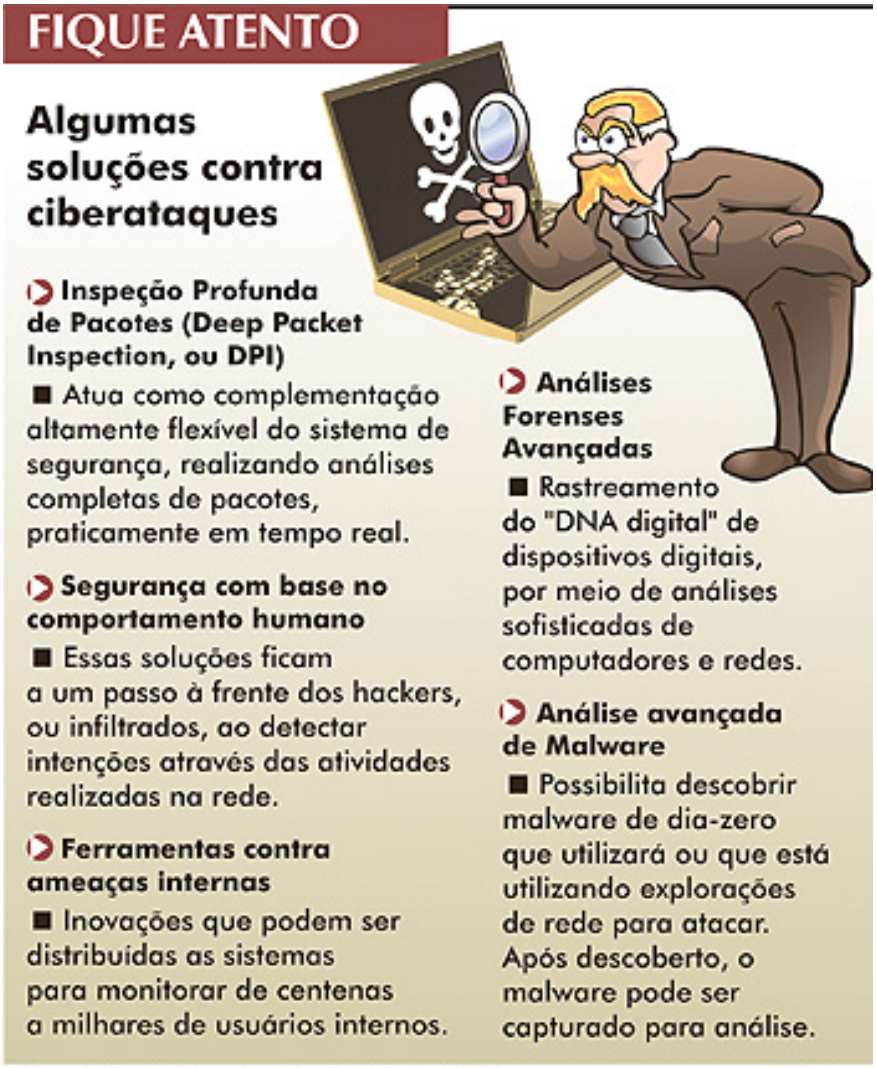
Andréa Bertoldi

O *site* do Dr. Omar Kaminski, advogado citado na reportagem, é o Internet Legal.

Segue a reportagem:

Cibercriminosos perceberam que pode ser bem mais vantajoso vender dados como segredos comerciais do que ficar caçando internautas descuidados na rede.

Segundo Christian Bachmann, especialista em segurança da informação, a ideia dos cibercriminosos é obter conteúdo e depois usá-lo contra as vítimas.



Curitiba – No submundo invisível do cibercrime, o roubo de capital intelectual corporativo – informações confidenciais de empresas – é atualmente o alvo predileto dos criminosos virtuais. Eles perceberam que pode ser bem mais vantajoso vender dados como segredos comerciais, planos de *marketing*, pesquisa e desenvolvimento para empresas concorrentes e governos estrangeiros do que ficar caçando internautas descuidados na rede.

Muitas vezes, acontece o roubo, mas as empresas não conseguem achar a origem e descobrir todos os dados que vazaram. Segundo o especialista em segurança da informação, Christian Bachmann, os principais focos de interesse dos cibercriminosos são projetos confidenciais e informações pessoais sobre donos das empresas. A ideia é obter as informações e depois usá-las contra as vítimas. Ele disse que uma situação comum é invadir um servidor da empresa e monitorar *e-mails*. Outro caso é entrar em computadores de funcionários e localizar senhas até ter acesso ao servidor.

Bachmann contou que um de seus clientes conversou com o contador por *e-mail* e teve os dados roubados. Essas informações foram usadas pelo sindicato dos trabalhadores que representava os funcionários da empresa para pedir aumento salarial e deflagrar uma greve.

O especialista citou algumas formas de prevenir problemas de roubo de capital intelectual. A primeira delas é realizar a atualização do sistema, ou seja, do servidor. Outra recomendação é criar uma rede separada para alguns servidores com o objetivo de ampliar a segurança, a chamada "DMZ". A presença de um antivírus em todos os computadores é uma prevenção básica.

Além disso, outra dica importante é melhorar a política de senhas dos funcionários e ter uma rede "VPN", uma rede virtual privada e mais fechada, com criptografia e mais difícil de ser acessada por pessoas estranhas. A rede *wireless* (rede sem fio) também deve ter criptografia e autenticação. "Algumas empresas têm mecanismos de segurança e outras esperam o problema acontecer para apagar o incêndio", alertou o advogado especializado em tecnologia, Omar Kaminski.

Ele disse que, em algumas situações, os funcionários podem "colaborar" com o roubo de informações por terem má índole ou por descontentamento, quando querem se vingar da empresa. Há ainda casos que têm a presença do "insider" quando, através da internet, uma pessoa rouba informações por meio de um amigo que é funcionário da empresa. "Muitas vezes a preocupação maior é em relação aos próprios funcionários", disse. Há companhias que fazem um termo de confidencialidade com o empregado para que ele responsabilize pelas informações e, em caso de descumprimento, são impostas sanções como multas.

Kaminski disse que é fundamental as empresas terem uma postura pró-ativa e "resguardar o capital intelectual que, muitas vezes, é mais importante que o capital físico". "O prejuízo pode ser tão grande a ponto de inviabilizar a atividade da empresa", disse. Por isso, é importante fazer um levantamento do ativo intelectual dentro da própria empresa.

Para ele, a prevenção inclui políticas de segurança de informações, termo de confidencialidade, política de privacidade, uso de criptografia e cuidado para guardar dados pessoais de clientes.

* A Folha de Londrina publicou a matéria "**Capital intelectual**: novo alvo dos crimes virtuais" no dia 26 de maio de 2011, entrevistando o Eng. Christian Bachmann da BS Brasil. A reportagem é sobre invasão digital, com foco no roubo de informações.

FONTE: BERTOLDI, Andréa. Folha de Londrina. Capital intelectual: novo alvo dos crimes virtuais. Entrevista de 26 de maio de 2011. Disponível em: <http://blog.bsbrasil.com.br/?p=194>. Acesso em: 9 jul. 2013.

RESUMO DO TÓPICO 3

Caro(a) acadêmico(a)! Neste terceiro tópico, você estudou os seguintes aspectos:

- Os diversos recursos implementados a fim de garantir a segurança da informação nos sistemas distribuídos.
- A definição de invasor, responsável pelos possíveis ataques nas informações que trafegam nos sistemas distribuídos.
- As ameaças que podem ocorrer aos processos e aos canais de comunicação e as formas de anulá-las.
- As ameaças de negação de serviço e código móvel que são utilizadas para romperem as atividades dos processos.
- A importância no uso dos modelos de segurança.

AUTOATIVIDADE

1 Com os avanços trazidos pela internet, muitas empresas passaram a utilizar esta ferramenta para realizar suas transações comerciais. Ocorre que, atualmente esse meio de comunicação e muito suscetível a invasões, podendo acarretar desta forma em sérios problemas aos seus usuários. A técnica de criptografia é uma das formas de anular esta ameaça, que consiste em algoritmos que utilizam chaves secretas, impedindo desta forma que a mensagem seja lida por alguém que não possua a chave de descriptografia correspondente.

( ) CERTO.
( ) ERRADO.

2 É um tipo de ataque que visa deixar os recursos de um sistema indisponíveis para seus usuários, através de inúmeras requisições de acesso.

a) ( ) Falsidade.
b) ( ) Negação de serviço.
c) ( ) Análise de tráfego.
d) ( ) Repetição.

Assista ao vídeo de resolução da questão 2

UNIDADE 2

PLANOS E POLÍTICA DA INFORMAÇÃO

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, será possível:

- conhecer os planos de segurança mais importantes e utilizados em um ambiente corporativo, os objetivos e elementos que devem estar presentes em cada um destes;
- entender a importância da formalização dos procedimentos em documentos que regulamentam o dia a dia da segurança dentro das corporações, assim como os planos utilizados quando da ocorrência de incidentes relacionados à quebra de segurança de tais controles;
- compreender a importância da política da informação, os elementos que devem constar de uma política de segurança, e os procedimentos para criação, implementação e acompanhamento de políticas de segurança.

PLANO DE ESTUDOS

Esta unidade está dividida em três tópicos, sendo que ao final de cada um deles, você encontrará atividades que auxiliarão na apropriação dos conhecimentos.

TÓPICO 1 – PLANO DE CONTINUIDADE OPERACIONAL

TÓPICO 2 – PLANO DE CONTINGÊNCIA

TÓPICO 3 – POLÍTICA DE SEGURANÇA

Assista ao vídeo desta unidade.

TÓPICO 1

PLANO DE CONTINUIDADE OPERACIONAL

1 INTRODUÇÃO

As organizações, quando criadas, têm a expectativa de permanecer desenvolvendo suas atividades durante muitos anos. Ou melhor, de fazê-lo indefinidamente. Os acionistas investem recursos com o objetivo de que a organização permaneça ativa e possibilite o retorno desse investimento.

Mesmo as entidades governamentais e as organizações sem fins lucrativos desejam permanecer no mercado a que se propuseram. Esse tipo de organização também oferece retorno aos seus acionistas, mas de uma forma diferente: retribuição social aos cidadãos, serviços prestados à população, melhoria de vida e ações que fortalecem a cidadania.

Em resumo, toda organização deseja continuar "viva", atuar no segmento escolhido, alcançar seus objetivos e cumprir sua missão.

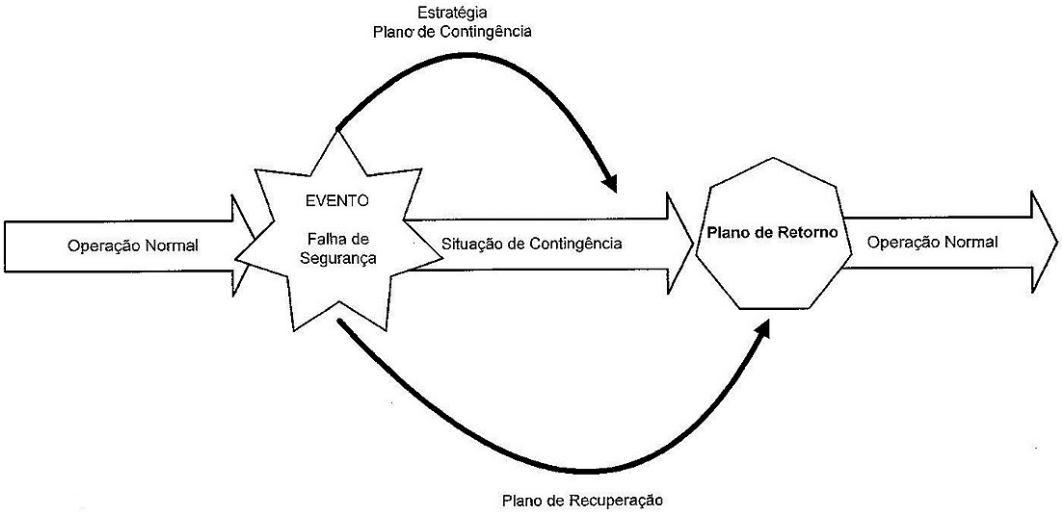
Como viver significa enfrentar riscos, para as organizações isso também é válido. Uma organização não deve deixar de existir porque uma situação de exceção aconteceu no seu dia a dia.

FONTE: Fontes (2006, p. 59)

> Garantir a continuidade de processos e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre. Com este propósito e formado pelas etapas de análise de impacto no negócio, estratégias de contingência e três planos de contingência propriamente ditos, o Plano de Continuidade de Negócios deve ser elaborado com o claro objetivo de contingenciar situações e incidentes de segurança que não puderem ser evitados. Deve ser eficaz como o paraquedas reserva o é em momento de falha do principal, garantindo, apesar do susto, a vida do paraquedista em queda. (SÊMOLA, 2003, p. 98).

Segundo o DRI – *Disaster Recovery Institute*, "de cada cinco empresas que possuem interrupção nas suas operações por uma semana, duas fecham as portas em menos de três anos". (SÊMOLA, 2003, p. 99).

FIGURA 18 – PAPÉIS DO PLANO DE CONTINGÊNCIA, PLANO DE RETORNO E PLANO DE RECUPERAÇÃO



FONTE: Sêmola (2003, p. 99)

Assim, o Plano de Continuidade tem, por sua natureza, um alto nível de complexidade, podendo assumir diversas formas em função do objeto a ser contingenciado e a abrangência de sua atuação. Diferente do que muitos imaginam, uma empresa não possuirá um plano único, mas diversos planos integrados e focados em diferentes perímetros, sejam físicos, tecnológicos ou humanos e, ainda, preocupada com múltiplas ameaças potenciais. Esta segmentação é importante; afinal, uma empresa tem processos cuja tolerância à falha é variável, os impactos idem, assim como o nível de segurança necessário à natureza das informações manipuladas (SÊMOLA, 2003).

> No caso da informação, cada organização deve estar preparada para enfrentar situações de contingência e de desastre que tornem indisponíveis recursos que possibilitam seu uso. Anteriormente, falamos da criação e manutenção de cópias de segurança, que é um procedimento básico para a organização enfrentar situações de contingência. É básico, mas não é suficiente porque, para que uma organização se recupere de uma situação de contingência e continue funcionando de forma adequada, também são necessários outros recursos: humanos, de tecnologia, de conhecimento dos processos, de ambiente físico e de infraestrutura. (FONTES, 2006, p. 59).

De acordo com Sêmola (2003, p. 104), "o Plano de Continuidade Operacional (PCO) tem como propósito definir os procedimentos para contingenciamento dos ativos que suportam cada um dos processos de negócio, tendo como objetivo reduzir o tempo de indisponibilidade e, consequentemente, os potenciais impactos para o negócio". Orientar as ações diante da queda de uma conexão à internet é um dos exemplos que podem ser citados para demonstrar os desafios organizados pelo plano.

Já conforme Imoniana (2011, p. 79), "possui o objetivo de assegurar que existem planos para diminuir os impactos de desastres que resultam na interrupção das operações normais da organização devido à falta de sistemas de informações".

2 PLANEJAMENTO DA CONTINUIDADE DO NEGÓCIO

A perda de acesso às informações ou à infraestrutura de tecnologia da informação representa um risco concreto e uma ameaça aos negócios. Todo gestor e membro da administração da organização se perguntam: o que a minha empresa faz para se proteger de ações ou fenômenos naturais ou provocados pela mão do homem? Qual a capacidade de continuar a operar ou se recuperar no caso de um evento de maior ou menor monta que impacte os negócios da empresa?

É função da administração em primeira instância e do Security Officer por consequência dar respostas a essas perguntas. Planos de recuperação de desastres e de continuidade de negócios devem existir para tranquilizar os gestores a respeito desses riscos. A boa governança corporativa, de T.I. e de Segurança da Informação devem zelar para que a organização dedique recursos e tempo no estudo e na preparação desses planos.

FONTE: Ferreira e Araújo (2008, p. 192)

As políticas de continuidade dos negócios, segundo Imoniana (2011, p. 79) "proveem alternativas para o processamento de transações econômicas e financeiras das organizações em casos de falhas graves de sistemas ou desastres". Esse plano deve ser monitorado e testado periodicamente para garantir sua prontidão para operar.

Também conhecidas por BCP (*Business Continuity Plan*) incluem, de acordo com Imoniana (2011, p. 79), procedimentos como:

- A gerência deve identificar suas informações críticas, níveis de serviços necessários e o maior tempo que poderia ficar sem o sistema.
- A gerência deve assinalar prioridades aos sistemas de informações para que possa determinar as necessidades de *backup* e sua periodicidade.
- O BCP deve ser desenvolvido e documentado e ter as manutenções atualizadas para garantir as operações pós-desastres.

Seja qual for o objeto da contingência – uma aplicação, um processo de negócio, um ambiente físico e, até mesmo, uma equipe de funcionários –, a empresa deverá selecionar a estratégia que melhor conduza o objeto a operar sob nível de risco controlado. Apesar de uma base conceitual comum, muitas são as variantes

de metodologia para a elaboração de um plano de continuidade; portanto, você pode se deparar com outras nomenclaturas ou novos grupamentos de estratégia. De qualquer forma, as soluções de continuidade vão sendo personalizadas de acordo com o contexto, pelas características de um segmento de mercado ou fato específico, como ocorreu no ano de 1999 por conta dos computadores com dificuldades de gerenciar a representação de data, apelidado de "*Bug* do Ano 2002". (SÊMOLA, 2003, p. 99).

De acordo com Ferreira e Araújo (2008, p. 111), "a política deve assegurar a existência de um plano de continuidade capaz de orientar todo o processo de restauração parcial ou total do ambiente de sistemas, incluindo também as atividades de teste e manutenção do plano".

Segundo Sêmola (2003, p. 104), "o Plano de Continuidade Operacional tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, consequentemente, os impactos potenciais ao negócio". Orientar as ações diante da queda de uma conexão à internet, exemplificam os desafios organizados pelo plano.

Conforme Imoniana (2011, p. 192), "visa proporcionar à gestão as interpretações do mapa cognitivo do ambiente operacional no que diz respeito às propensões das ameaças e vulnerabilidades de uma organização de modo a facilitar a antecipação das vantagens que porventura possam ser identificadas no momento atual de uma empresa".

É a habilidade de se assegurar a continuidade de desenvolvimento de produtos ou serviços e apoios aos consumidores de forma ininterrupta e manter a viabilidade corporativa após uma exposição a um desastre (IMONIANA, 2011).

Segundo Imoniana (2011, p. 192), "o BCP prepara uma organização de forma planejada na tentativa de melhor enfrentar incidentes dos processos operacionais que poderiam arriscar as missões empresariais e, sobretudo, a saúde financeira".

A gestão de TI, conforme Ferreira e Araújo (2008, p. 111), "deve obter colaboração dos gestores de negócio, criando diretrizes de continuidade referendadas pelos mesmos, de forma a definir claramente os papéis e responsabilidades, e aprovação dos critérios para a análise de impacto (BIA)".

O desenvolvimento e a implementação de BCP, de acordo com Imoniana (2011, p. 192), "partem da premissa de que o cliente precisa ser atendido custe o que custar". Entendendo que o lema de quase todas as empresas hoje é cliente em primeiro lugar, ele não poderá ser prejudicado por falta de produtos ou serviços quando da ocorrência de um imprevisto do processo operacional e da consecução dos objetivos dos negócios. Assim, o BCP deve ser efetivo a ponto de prover as atividades normais das organizações.

O teor do capítulo de gestão da continuidade e/ou contingência, na política, deve abordar diversos aspectos com relação à avaliação de risco e impacto no negócio (BIA). "A política deve ressaltar que, o plano ao ser desenvolvido, resultará num conjunto de documentos onde estarão registradas as ações relativas às adequações da infraestrutura e às alterações dos procedimentos". (FERREIRA; ARAÚJO, 2008, p. 111).

Na política, ainda segundo Ferreira e Araújo (2008, p. 111), deve-se detalhar que o Plano de Contingência e/ou Continuidade seja revisado e testado periodicamente de forma a garantir o seu funcionamento em caso de necessidade. Os riscos que serão minimizados com a criação de um plano aderente à política de segurança incluem, mas não se limitam a:

- Comprometimento das operações com os clientes.
- Perda de receita e vantagem competitiva perante a concorrência.
- Multas e sanções legais.

De acordo com Ferreira e Araújo (2008, p. 111-112), "os trabalhos relativos à contingência de sistemas e/ou continuidade do negócio devem estar integrados com a gestão de riscos do negócio e de TI, de forma que eventuais riscos mapeados estejam parcialmente ou totalmente suportados".

BCP, de acordo com Imoniana (2011, p. 192-193), "tem o objetivo de assegurar quaisquer impedimentos que possam colocar em jogo os postulados de Continuidade, simplesmente conhecido por *Going-Concern*. Este postulado de contabilidade afirma que a entidade (a empresa) é um organismo vivo que irá viver por um período de tempo indeterminado até que surjam fortes evidências provando o contrário". As abrangências são:

- Organismos que renovam suas células vivas através do processo de reinvestimentos; e
- Produtor de riqueza e gerador de valores continuadamente.

Os trabalhos de avaliação de impacto devem servir como entrada para os trabalhos de gestão de riscos, da mesma forma que os resultados deste último devem subsidiar a gestão de continuidade (FERREIRA; ARAÚJO, 2008).

> Se indagássemos por que *Business Continuity Planning*, hoje seria uma ingenuidade, uma vez que vivenciamos uma época muito tumultuosa, cheia de ameaças, vulnerabilidades e riscos, sejam eles de nível país ou organizacional. Aliadas às causas naturais, haja vista as provocadas pela desestabilização da temperatura terrestre como inundações, tufões, terremotos, El Niño, ciclones, tsunamis, só para citar alguns. (IMONIANA, 2011, p. 193).

Ferreira e Araújo (2008, p. 112) citam que o processo de gestão da continuidade deve prover pelo menos as seguintes atividades de controle:

- Assegurar que um plano formal (escrito) esteja desenvolvido, testado e amplamente divulgado (incluindo treinamento).
- Procedimentos de urgência/emergência descritos e testados.
- Procedimentos corretivos e de recuperação desenhados para trazer os negócios de volta à posição em que se encontravam antes do incidente ou desastre.
- Ações para salvaguardar e reconstruir o site original.
- Procedimentos para interação com as autoridades públicas; e
- Comunicação com funcionários, clientes, fornecedores, acionistas, alta administração, autoridades públicas e imprensa.

Geralmente, as empresas de auditoria independentes executam os serviços de avaliação de BCP como atividade à parte e não se enquadram nos escopos de tarefas de exames focados para obtenção de confianças para que se possam emitir os pareceres de auditoria. Ou seja, auditoria dos controles gerais de sistemas e de tecnologia de informações aliada ao processo de testes de controles, avaliação de sistemas aplicativos aliado ao teste substantivo e analíticos substantivos ou das revisões limitadas (IMONIANA, 2011).

Para garantir a eficiência do Plano de Continuidade de Negócios é preciso construir um processo dinâmico de manutenção e gestão de todos os documentos, garantindo a integração e a eficácia em situações de desastre. Desenvolver o plano a partir de uma Análise de Riscos prévia é a melhor forma de aumentar a eficácia e o retorno sobre os investimentos (SÊMOLA, 2003).

3 IDENTIFICAÇÃO DOS PROCESSOS CRÍTICOS

Em ambientes de informações e informática, de acordo com Caruso e Steffen (1999, p. 70), "temos duas classes principais de materiais em processo, a saber: o acervo de informações destinadas a confeccionar as ferramentas de processamento de informações ou sistemas de programas de aplicações ou de controle da atividade e informações relacionadas com as atividades dentro das empresas, que serão processadas pelos sistemas informatizados".

Além disso, ainda segundo Caruso e Steffen (1999, p. 70), "temos que ter sempre em conta que não existe informação sem custo; mesmo em casos em que as informações são obtidas sem nenhum custo, a estrutura organizacional e de recursos necessária para a coleta tem um custo, que é rateado em cima de cada unidade de informação coletada".

O processo inicia-se por uma análise de riscos e de impactos aos negócios, o chamado BIA, que irá mapear os processos de negócios, medir o tempo máximo aceitável de parada de cada um desses processos e então traçar as estratégias de recuperação e continuidade para cada processo (FERREIRA; ARAÚJO, 2008).

4 ANÁLISE E CLASSIFICAÇÃO DOS IMPACTOS

Conhecido mundialmente pela sigla BIA – *Business Impact Analysis*, esta primeira etapa é fundamental por fornecer informações para o perfeito dimensionamento das demais fases de construção do plano de continuidade. Seu objetivo é levantar o grau de relevância entre os processos ou atividades que fazem parte do escopo da contingência em função da continuidade do negócio. Em seguida, são mapeados os ativos físicos, tecnológicos e humanos que suportam cada um deles, para então apurar os impactos quantitativos que poderiam ser gerados com a sua paralisação total ou parcial (SÊMOLA, 2003).

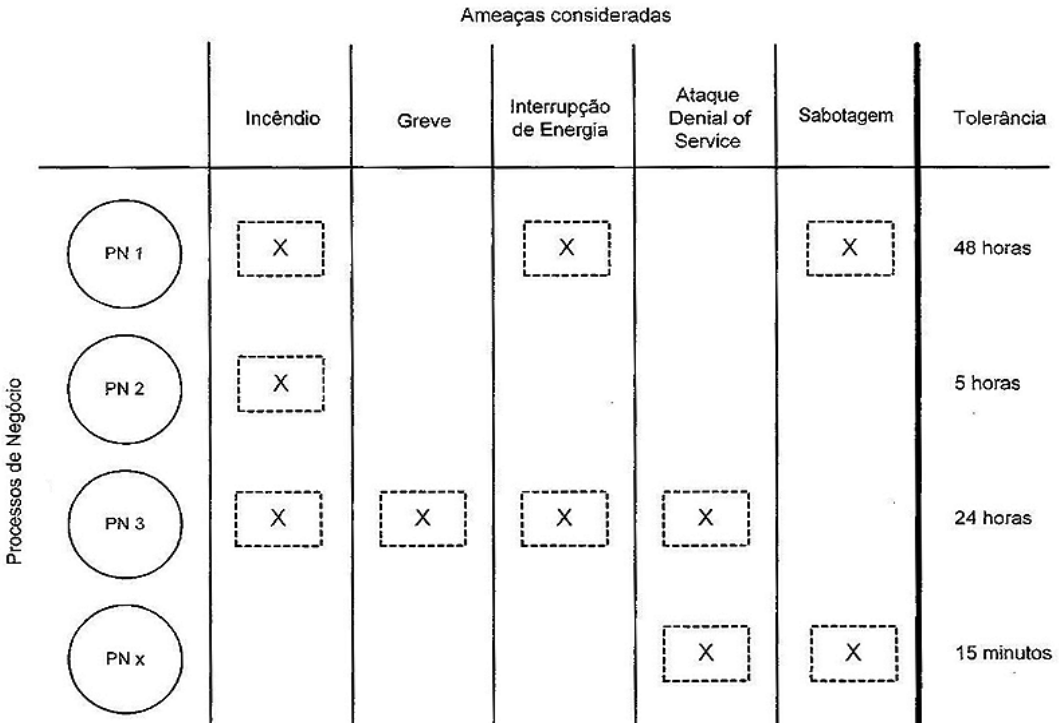
QUADRO 10 – RELEVÂNCIA ENTRE PROCESSOS PERTENCENTES AO ESCOPO DO PLANO

Processos de Negócio Escala		**PN1**	**PN2**	**PN3**	**PN4**	**PNn**
1	Não considerável					
2	Relevante	X				
3	Importante			X		
4	Crítico				X	
5	Vital		X			

FONTE: Adaptado de Sêmola (2003, p. 100)

> De posse desta análise BIA, torna-se possível definir as prioridades de contingência, os níveis de tolerância à indisponibilidade de cada processo ou atividade pertencente à contingência e, ainda, agrupar os ativos em função de sua natureza e relação de dependência que mantêm com os processos. Tem-se, a partir de então, uma fotografia de funcionalidade dos processos, restando definir as ameaças que se quer contingenciar. A escolha das ameaças a se considerar para cada processo está diretamente ligada à probabilidade e severidade de um incidente. (SÊMOLA, 2003, p. 100).

FIGURA 19 – AMEAÇAS CONSIDERADAS E PERCEPÇÃO DE TOLERÂNCIA DOS PROCESSOS DE NEGÓCIOS



FONTE: Sêmola (2003, p. 101)

De acordo com Sêmola (2003, p. 100-101), "percebe-se que muitas das tarefas realizadas pelo BIA poderiam ser complementadas pelos resultados de uma análise de riscos, sendo esta, portanto, a atividade primeira e mais importante para orientar todas as ações de segurança da informação. Se esta herança ocorresse efetivamente, o BIA se resumiria a quantificar os impactos e a selecionar as ameaças a serem consideradas pelo plano de continuidade do negócio". (consulte a figura 19).

De acordo com Ferreira e Araújo (2008, p. 177), "o melhor modo de determinar o grau de risco é relacionar detalhadamente quais seriam os impactos para a organização se uma ameaça conseguir explorar uma vulnerabilidade".

Antes de iniciar uma análise de impacto, de acordo com os autores, é necessário ter em mãos as informações obtidas por meio da documentação dos sistemas, bem como de relatórios já existentes de avaliações de impactos anteriormente realizados. Os resultados determinam o impacto na organização caso os sistemas sejam comprometidos, baseados em avaliação qualitativa e quantitativa. Uma avaliação de criticidade identifica os principais ativos (ex.: *hardware*, *software*, sistemas, serviços e etc.) que suportam as atividades da organização.

Se estas documentações não existirem ou avaliações de impacto nunca tiverem sido realizadas, a criticidade dos sistemas pode ser determinada em nível de proteção necessária para manter a confidencialidade, integridade e disponibilidade.

Apesar dos métodos utilizados para determinar a criticidade dos sistemas e de suas informações, seus proprietários são os únicos responsáveis pela exata determinação do nível de impacto que a organização estará sujeita caso a confidencialidade, integridade e disponibilidade sejam comprometidas. Consequentemente, a realização de entrevistas com estes profissionais é indispensável.

Podemos concluir que, o impacto de um incidente de segurança pode ser descrito em termos de perda ou degradação de qualquer, ou combinação, das principais metas que devem ser alcançadas no contexto da Segurança da Informação: confidencialidade, integridade e disponibilidade.

FONTE: Ferreira e Araújo (2008, p. 177)

Alguns impactos podem ser medidos quantitativamente por meio da determinação da perda financeira e custo para realização de manutenção corretiva. Ferreira e Araújo (2008, p. 177) especificam no quadro a seguir as categorias de impacto que poderão ser utilizadas:

QUADRO 11 – CATEGORIAS DE IMPACTO

NÍVEL	**DEFINIÇÃO**
Alto	• Perda significante dos principais ativos e recursos. • Perda da reputação, imagem e credibilidade. • Impossibilidade de continuar com as atividades de negócio.
Médio	• Perda dos principais ativos e recursos. • Perda da reputação, imagem e credibilidade.
Baixo	• Perda de alguns dos principais ativos e recursos. • Perda de reputação, imagem e credibilidade.

FONTE: Adaptado de Ferreira e Araújo (2008, p. 177)

5 DESENVOLVIMENTO E DOCUMENTAÇÃO DO PLANO

Para que as empresas possam estar prontas para atender problemas de paradas inesperadas que poderiam abalar a continuidade de seus negócios, Imoniana (2011, p. 193-194) recomenda que o BCP abranja os seguintes itens:

- Plano de Reinicialização de Negócios (*Business Resumption Planning – BRP*): caracteriza-se por processo de desenvolvimento de compromissos e agenda de procedimentos que garanta à organização corresponder ao evento indesejado de tal forma que as funções essenciais consideradas críticas para os negócios continuem sendo operadas em conformidade com os níveis planejados e também mantendo um nível esperado de perdas sem surpresas.

- Gestão de Crises (*Crisis Management – CM*): nomeação da coordenação efetiva e global para a busca de respostas às crises de forma pontual e em tempo hábil a fim de minimizar os efeitos na lucratividade, imagem corporativa e o diferencial da organização.
- Plano de Recuperação de Tecnologia e Sistemas de Informação (*IT Disaster Recovery – DR*): caracteriza-se pelos planos desenhados para manter os níveis de apoio de sistemas e tecnologia de informação no processo de gestão. Restaura informações, comunicação e sistemas em condições aceitáveis, minimizando, assim, as perdas financeiras no processo de desenvolvimento de produtos ou serviços.
- Teste de emergência e de recuperação (*Emergency Preparedness* – EP): caracteriza-se pelo teste periódico da preparação para enfrentar o pior que vier. Para que a gerência possa se posicionar no tocante à manutenção das atividades devem-se executar de tempo em tempo testes para simular desastres e se disciplinar quanto às falhas deste processo.

6 TREINAMENTO E CONSCIENTIZAÇÃO DO PESSOAL

Os recursos humanos são considerados o elo mais frágil da corrente, pois são responsáveis por uma ou mais fases de processo de segurança da informação. Esta situação é ratificada pelo fato de o *peopleware* não ter um comportamento binário e previsível em que se possam eliminar todas as vulnerabilidades presentes. O ser humano é uma máquina complexa, dotada de iniciativa, criatividade e que sofre interferência de fatores externos, provocando comportamentos nunca antes experimentados. O fator surpresa é um dos pontos nevrálgicos dos processos de segurança que dependem das pessoas. Se especificarmos normas de criação, manuseio, armazenamento, transporte e descarte de senhas, implementamos recursos tecnológicos de auditoria e autenticação de acesso para tornar um ambiente mais seguro, podemos ter a eficiência dessas iniciativas postas em dúvida à medida que um recurso humano descumpra as instruções da política de segurança e compartilhe sua senha supostamente pessoal e intransferível (SÊMOLA, 2003).

Peopleware são as pessoas que trabalham diretamente, ou indiretamente, com a área de tecnologia da informação, ou mesmo com Sistema de Informação. É a parte humana que se utiliza das diversas funcionalidades dos sistemas computacionais, seja este usuário um Analista de Sistema ou, até mesmo, um simples cliente que faz uma consulta em um caixa eletrônico da Rede Bancária, como também uma atendente de um Supermercado.

FONTE: Disponível em: <http://pt.wikipedia.org/wiki/Peopleware>. Acesso em: 13 jul. 2013.

Esses riscos precisam ser tratados de forma gradativa, objetivando formar uma cultura de segurança que se integre às atividades dos funcionários e passe a ser vista como um instrumento de autoproteção. As ações devem ter a estratégia de compartilhar a responsabilidade com cada indivíduo, transformando-o em coautor do nível de segurança alcançado. Somente dessa forma as empresas terão, em seus funcionários, aliados na batalha de redução e administração dos riscos.

Muitas são as formas de iniciar a construção da cultura de segurança. Algumas delas se aplicam a públicos com perfis diferentes; outras se aplicam a todos os perfis, mas em momentos distintos.

O trabalho deve começar com seminários abertos voltados a compartilhar a percepção dos riscos associados às atividades da empresa, os impactos potenciais no negócio e, principalmente, o comprometimento dos processos críticos se alguma ameaça se concretizar. Desta forma, cada funcionário passa a se enxergar como uma engrenagem da máquina e corresponsável por seu bom funcionamento, podendo gerar impactos diretos ao seu processo e indiretos a processos adjacentes.

FONTE: Sêmola (2003, p. 130)

O nível de segurança de uma corrente é equivalente à resistência oferecida pelo elo mais fraco. O *peopleware* representa justamente esse elo; por isso, deve ser alvo de um programa contínuo e dinâmico, capaz de manter os recursos humanos motivados a contribuir, conscientes de suas responsabilidades e preparados para agir diante de antigas e novas situações de risco (SÊMOLA, 2003).

Por conta disso, Sêmola (2003, p. 130-131) "sugere que seja feita uma campanha de divulgação, que deverá lançar mão de diversos artifícios para comunicar os padrões, critérios e instruções operacionais, como cartazes, jogos, peças promocionais, protetores de tela, *e-mails* informativos, *e-mails* de alerta, comunicados internos, páginas especializadas na Intranet etc.".

De acordo com Sêmola (2003, p. 131-132), "dentro do quadro de funcionários, existem perfis profissionais que necessitam de maior domínio dos conceitos, métodos e técnicas de segurança, podendo inclusive, variar sua área de interesse e profundidade". Os administradores de rede, por exemplo, precisam estar preparados para reagir às tentativas de ataque e invasão, ou para contingenciar situações de risco. O *Security Officer*, por sua vez, deve ter condições de definir, medir e avaliar os índices e indicadores de segurança para subsidiar seus planos de gestão e seu planejamento de trabalho, a fim de garantir a total integração das ações e, principalmente, alcançar os objetivos.

O *Security Officer*, atuando como eixo central na função de Coordenação Geral do Comitê Corporativo de Segurança da Informação, tem papel substancial para o sucesso do modelo. É ele quem recebe toda a pressão da empresa diante dos resultados e quem é demandado a adequar o nível de controle, e, portanto, o nível de segurança para suprir as novas demandas do negócio.

FONTE: Sêmola (2003, p. 63)

> Para todos esses casos, não bastam os seminários e campanhas de conscientização. Eles precisam de capacitação formal através de cursos especializados, que propõem uma certificação como instrumento de reconhecimento da competência. Pela heterogeneidade de perfis, surgem demandas de cursos verticalmente técnicos, voltados a capacitar recursos em uma determinada tecnologia de segurança, bem como demandas para orientação e preparação de *Security Officers*. Entretanto, é relevante destacar a necessidade de processos contínuos de sensibilização e capacitação das pessoas, sob pena de ter a equipe estagnada e, brevemente, despreparada para a administração das novas situações de risco. (SÊMOLA, 2003, p. 132).

7 TESTE DO PLANO

De acordo com Imoniana (2011, p. 194), os objetivos da auditoria de *Business Continuity Planning* compreendem:

1) Certificar-se da integridade das estratégias mantidas pela alta gestão para enfrentar situações de desastre ou de risco de descontinuidade das operações.
2) Certificar-se das normas de BCP e se as regras contidas nelas são válidas e são homogeneamente disseminadas para todos os integrantes da alta cúpula e também para as pessoas que precisam saber dos planos da instituição a fim de atender vários níveis de estragos que poderiam comprometer a imagem da organização.
3) Certificar-se das responsabilidades para os processos e ações delineadas de forma específica e em equipe.
4) Certificar-se de que sistemas de informações, tecnologias e processos de comunicação estão preparados para eventuais riscos de continuidades.
5) Certificar-se de que os processos de documentação da transação de BCP registrados junto ao coordenador de gestão de crises de continuidade e os membros que constituem a força-tarefa de continuidade são válidos e íntegros.

O quadro a seguir demonstra um programa de avaliação de *Business Continuity Planning*, segundo Imoniana (2011, p. 195-197):

QUADRO 12 – PROGRAMA DE AVALIAÇÃO DE *BUSINESS CONTINUITY PLANNING*

Nº	Controles/Procedimentos de Testes	S / N / NA	Obs.
C1 – As funções de Gestão de Crises de Continuidades são delineadas?			
	P1 – Existe a função da pessoa a quem se deve recorrer quanto às questões de continuidade?		
	P2 – Quem é a pessoa? - Gerente de controladoria - Gerente Administrativo/Financeiro - Gerente de Operações - Gerente de Vendas - Gerente de Crises - Gerente de Risco - Consultor Externo - Outro, citar _____.		
	P3 – Verifique junto à pessoa que descreva sucintamente sua atribuição e a periodicidade da atuação.		
C2 – Os funcionários são conscientizados a respeito da importância estratégica de BCP?			
	P1 – Efetuar reuniões periódicas para transmitir questões de continuidade para os funcionários.		
	P2 – Verificar as agendas de reuniões para certificar desta atividade de BCP.		
C3 – Com qual prazo se podem obter informações e orientações sobre a continuidade das operações? ***Teste de Validade***			
	P1 – Certificar-se entre os prazos a seguir para obter dados sobre continuidade: - 24 horas - 1 semana - 10 dias - 30 dias - Outros, citar_____		
	P2 – Somente as pessoas autorizadas possuem acesso?		

	P3 – Selecione aleatoriamente o registro de pessoas documentadas para constatar a procedência do cadastro e verifique as consistências a fim de nos assegurarmos da integridade.		
	P4 – Selecione um integrante da equipe de gestão de continuidade para certificar-se da validade de alocação das tarefas e sua compatibilidade.		
C4 – A empresa possui um banco de dados onde todas as orientações quanto aos possíveis problemas de continuidade são contempladas e as respostas apontadas? (*Teste de Integridade*)			
	P1 – As informações que explicam o BCP são genéricas?		
	P2 – As informações que explicam as estratégias e os componentes de tais estratégias são detalhadas?		
	P3 – Verificar através de observação e indagações corroborativas acessando o sistema para comprovar informações úteis registradas sobre BCP e classificá-lo entre: irrelevante, baixo, moderado, significativo, muito significativo.		
C5 – Testa periodicamente os componentes de BCP pelo menos uma vez por ano?			
	P1 – Quando foi feito o teste pela última vez?		
C6 – Treinamento de equipes de BCP é feito periodicamente e a cargo de quem?			
	P1 – Verificar o cronograma de treinamentos dos funcionários a respeito de BCP e concluir a respeito da razoabilidade.		
C7 – Como se faz para exercitar a prontidão do BCP para atender às possibilidades planejadas?			
	P1 – Quando foi feito o último exercício de prontidão para enfrentar ameaças por meio de testes?		
	P2 – Está programado o próximo teste de prontidão de BCP? Quem vai dar o *start up*?		
C8 – Existem controles efetuados pelo sistema de registro de eventos que garantam que este módulo se converse com o sistema de gestão de riscos empresariais a fim de gerar alertas? ***Interface Sistêmica***.			

	P1 – Verifique os controles programados para certificar-se da consistência entre interfaces de Sistemas de Gestão de Crises e Sistemas de Mapeamento das métricas de vulnerabilidades, ameaças e riscos.		
C9 – Manutenção e atualizações de BCP são feitas num intervalo fixo e pelo menos uma vez por ano?			
	P1 – Verificar através de análise documental ou documentação sistêmica para certificar-se da última atualização.		
	P2 – Como é feita a distribuição das atualizações?		
	P3 – Quem inclui as alterações e em que periodicidade?		
	P4 – Versões anteriores são destruídas? Como são feitas?		
	P5 – Quem efetua as destruições?		
C10 – Existe possibilidade de contratos de BCP que não estejam válidos a ponto de não cobrir época de sua ocorrência? (*Teste de Registro/Cut-off*).			
	P1 – Analisar o teor dos contratos de BCP a fim de constatar sua adequacidade.		
	P2 – Selecione aleatoriamente alguns contratos dentre as datas bases de auditoria para testes.		
C11 – Existe procedimento que propicie melhoria contínua por meio de emulação de *benchmarking*?			
	P1 – Verifique o procedimento de execução de *benchmarking* a fim de certificar-se da adequacidade.		

FONTE: Adaptado de Imoniana (2011, p. 195-197)

Fontes (2006, p. 60-61) coloca algumas perguntas que devem ser feitas, para reflexão:

1) Existe, na sua organização, um plano para a recuperação do negócio em caso de situações de desastre ou de contingência?
2) Você conhece esse plano?
3) Você já participou de um teste ou de uma simulação de situação de desastre?
4) Muitas vezes, pensamos que um acontecimento só será considerado desastre se afetar toda a empresa. Mas, se acontecer uma quebra ou roubo dos equipamentos de tecnologia, como ficará a execução do trabalho pelas pessoas desse departamento?
5) Existem outros recursos que são tão importantes quanto os recursos computacionais. Você seria capaz de identificá-los? Existe um plano de uso de recursos alternativos para esses casos?
6) Se alguma pessoa do seu grupo de trabalho estiver ausente da organização em uma situação de contingência, sua equipe conseguirá prosseguir na realização das tarefas operacionais e alcançar os objetivos de negócio dentro de um tempo adequado?
7) Se acontecer um incêndio no seu ambiente de trabalho, você saberá o que fazer? Vai precisar levar alguma coisa?
8) Os conceitos de continuidade são válidos para a vida pessoal. Por acaso já considerou sua continuidade profissional ou pessoal caso aconteça um desastre com você?

8 ATUALIZAÇÃO E MANUTENÇÃO DO PLANO

Ferreira e Araújo (2008, p. 160) "recomendam especificar procedimentos ou uma metodologia formal para a manutenção periódica e aprovação das políticas de forma a mantê-los atualizados frente a novas tendências, tecnologias e acontecimentos".

> O intervalo médio utilizado para a revisão da política é de seis meses ou um ano, porém deve ser realizada uma revisão sempre que forem identificados fatos novos, não previstos na versão atual que possam ter impacto na segurança das informações da organização.
>
> Adicionalmente, os demais comitês internos envolvidos, gestores de negócio, Tecnologia e Segurança da Informação devem estar atentos às modificações na estrutura da organização que possam eventualmente ter impacto na política e em seus procedimentos.

FONTE: Ferreira e Araújo (2008, p. 160)

O processo de revisão, segundo Ferreira e Araújo (2008, p. 160), deve abranger:

- Eventuais riscos identificados.
- Alterações na legislação do negócio.
- Incidentes de segurança.
- Vulnerabilidades encontradas.
- Alterações na estrutura organizacional; e
- Tendências do mercado.

Que tal assistir a outro grande filme, e ver como o governo norte-americano coloca em prática seu plano de contingência quando o país é vítima de um *ciber* ataque?

Doze anos após a aparição em Duro de Matar: A Vingança, John McClane (Bruce Willis) é convocado para a última missão: combater criminosos que atuam pela internet. Os terroristas planejam desligar todos os sistemas de computadores no feriado de 4 de julho, dia da independência dos Estados Unidos. A trama se passa em Washington, mas acompanha a velocidade das transmissões cibernéticas, englobando todo o território norte-americano na possível catástrofe.

Os Estados Unidos sofrem um novo ataque terrorista, desta vez através da informática. Um *hacker* consegue invadir a infraestrutura computadorizada que controla as comunicações, transporte e energia do país, ameaçando causar um gigantesco blecaute. O autor do ataque planejou todos os passos envolvidos, mas não contava que John McClane (Bruce Willis), um policial da velha guarda, fosse chamado para confrontá-lo.

DURO DE MATAR 4.0. Direção de Len Wiseman. EUA: Fox Filmes, 2007, DVD (128 min), color.

9 PRESERVAÇÃO DAS CÓPIAS DE SEGURANÇA

A disponibilidade do ambiente de processamento de dados é fundamental em qualquer organização, independentemente de seu tamanho e valor de suas receitas. (FERREIRA; ARAÚJO, 2008, p. 112).

"Para manter as informações disponíveis é necessário, além dos recursos de *hardware*, possuir procedimentos de *backup* e *restore* das informações. Estes por sua vez devem ser capazes de orientar as ações de realização e recuperação das informações". (FERREIRA; ARAÚJO, 2008, p. 112).

O valor da informação produzida na organização além do valor estratégico para o negócio é também a soma de inúmeras horas de trabalho no desenvolvimento de documentos, informações, produtos, entre outros esforços, que provavelmente em qualquer tentativa de quantificar seu valor, teremos um número aproximado, porém, dificilmente, exato e com grandes chances de, a cada cálculo realizado, ter valores diferentes. No entanto, é evidente que o procedimento de *backup* é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisação na ocorrência de um sinistro.

Para a implementação do *backup*, deve-se levar em consideração a importância da informação, o nível de classificação utilizado, sua periodicidade de atualização e também sua volatilidade.

FONTE: Ferreira e Araújo (2008, p. 113)

Com base nos conceitos apresentados acima, Ferreira e Araújo (2008, p. 113-114) entendem que a organização deve elaborar seus procedimentos com base nas seguintes premissas:

- Realizar *backups* visando diminuir os riscos da continuidade.
- Manter os *backups* em local físico distante da localidade de armazenamento dos dados originais.
- Realizar testes nas mídias que armazenam os *backups* para assegurar que os mantidos em ambiente interno e/ou externo estejam seguros e em perfeito estado para serem utilizados.
- Desenvolver e manter a documentação dos procedimentos de *backup* e *restore* sempre atualizada.
- Assegurar que seja mantido um inventário sobre as mídias que armazenam os *backups*.

De acordo com Ferreira e Araújo (2008, p. 114), a frequência para a realização dos *backups* e a respectiva retenção deve ser determinada considerando a velocidade e volatilidade da informação, ou seja, depende da periodicidade em que os dados são alterados. Portanto, para determinar a frequência e a retenção no procedimento de *backup*, considere os conceitos e as premissas a seguir:

- Velocidade da informação: periodicidade na qual a informação é atualizada.
- Volatilidade da informação: período de tempo no qual a informação permanece atual e utilizada. Por exemplo: para os dados que não sofrerem alteração pelo período de trinta dias, somente será necessária a realização de um novo *backup* no trigésimo primeiro dia, consequentemente, sua retenção programada poderá ser para trinta dias.

Esses dois conceitos devem orientar a frequência e retenção da realização dos *backups*. Por sua vez, de acordo com Ferreira e Araújo (2008, p. 114), "o armazenamento das mídias de *backup* deve ser realizado em localidade diferente de onde estão armazenados os equipamentos geradores da informação".

> A integridade dos *backups* é comprometida quando as mídias estão armazenadas juntamente com os equipamentos onde os dados estão sendo gerados. Desastres (incidente causado pela natureza, tais como, incêndios, terremotos ou incidente causado por atos maliciosos) poderão causar destruição ou danificação dos equipamentos e de seus *backups*, consequentemente, comprometendo o processo de reconstituição do ambiente. (FERREIRA; ARAÚJO, 2008, p. 114).

Além dos *backups* realizados por empresas terceiras, como, por exemplo, "provedores de *sites* de contingência, deve-se produzir uma cópia adicional de segurança dos *backups* considerados mais críticos para ser armazenada nas instalações da organização independentemente das cláusulas contratuais estabelecidas, que visam proteger a organização". (FERREIRA; ARAÚJO, 2008, p. 115).

Para todos os *backups* devem existir registros das operações envolvidas na ação de realizar a cópia. Ferreira e Araújo (2008, p. 115) sugerem constar as seguintes informações para os *backups* (diários, semanais, mensais e anuais):

- Nome do servidor: especificar o nome da mídia física utilizada no *backup* do servidor ou qualquer outro recurso gerador da informação.
- Quantidade total de fitas: detalhar a quantidade de fitas utilizadas nos casos aplicáveis.
- Tipo de mídia: especificar o recurso utilizado (CD, DVD, fita DAT, disquete etc.).
- Localização do servidor: registrar a localização do servidor.
- Descrição do conteúdo: descrever os arquivos, sistemas etc.
- Período de retenção: especificar o período de tempo em que as informações constantes na mídia devem ficar retidas para assegurar uma maior proteção ao negócio.
- Horário: descrever o horário em que a atividade de *backup* é realizada.
- Tipo: especificar o tipo de *backup* selecionado, como por exemplo, se é "*full*", *diferencial* ou *incremental*.
- Dependência: descrever as dependências de outras rotinas configuradas e agendadas.
- Instruções de trabalho: documentar a operação do *software* de *backup* com alto nível de detalhes, e se possível com o uso de cópias da tela do *software* utilizado.
- Restrições: descrever possíveis restrições que possam existir.

FIGURA 20 – MODELO DE ETIQUETA PARA AS MÍDIAS DE *BACKUP*

<Nome Empresa>

<Área>
Servidor: "ABC"

Backup Semanal
Data: dd/mm/aaaa
Hora: hh:mm
Código:
Descrição:

<Área>
Backup Semanal

FONTE: Adaptado de Ferreira e Araújo (2008, p. 116)

Os testes de restauração (*restore*) devem ser periódicos com o objetivo de garantir a qualidade dos *backups*, tendo por finalidade, segundo Ferreira e Araújo (2008, p. 116):

- Verificar a integridade da informação armazenada.
- Avaliar a funcionalidade dos procedimentos.
- Verificar a capacitação e a falta de treinamento da equipe.
- A identificação de procedimentos desatualizados ou ineficazes.
- A identificação de falhas ou defeitos.

RESUMO DO TÓPICO 1

Caro(a) acadêmico(a)! Neste tópico, você estudou que:

- O Plano de Continuidade tem, por sua natureza, um alto nível de complexidade, podendo assumir diversas formas em função do objeto a ser contingenciado e a abrangência de sua atuação.

- Não existe informação sem custo. Até mesmo em casos em que as informações são obtidas aparentemente sem nenhum custo, a estrutura organizacional e de recursos necessária para a coleta, demandam algum custo, cuja divisão é feita entre cada unidade de informação coletada.

- Antes de iniciar uma análise de impacto é necessário possuir as informações obtidas por meio da documentação dos sistemas, além dos relatórios já existentes de avaliações de impacto realizadas anteriormente.

- O melhor modo de determinar o grau de risco é relacionar detalhadamente quais seriam os impactos para a organização se uma ameaça conseguir explorar uma vulnerabilidade.

- Os riscos precisam ser tratados de forma gradativa, objetivando formar uma cultura de segurança que se integre às atividades dos funcionários e passe a ser vista como um instrumento de autoproteção.

- O intervalo médio utilizado para a revisão da política de segurança é de seis meses ou um ano, porém deve ser realizada uma revisão sempre que forem identificados fatos novos que possam ter impacto na segurança das informações da organização.

- Para a implementação do *backup*, deve-se levar em consideração a importância da informação, o nível de classificação utilizado, sua periodicidade de atualização e também sua volatilidade.

AUTOATIVIDADE

1 Cite três atividades de controle que o processo de gestão da continuidade deve prover.

2 Cite dois objetivos da auditoria de BCP (*Business Continuity Planning*).

3 Qual é a melhor forma de desenvolver o plano de continuidade de negócios de forma a aumentar a eficácia e o retorno sobre os investimentos?

4 Quais itens são recomendados que o BCP (*Business Continuity Planning*) abranja?

5 Quais fatores devem ser considerados na hora de implantar um plano de *backup*?

Assista ao vídeo de resolução da questão 2

TÓPICO 2

PLANO DE CONTINGÊNCIA

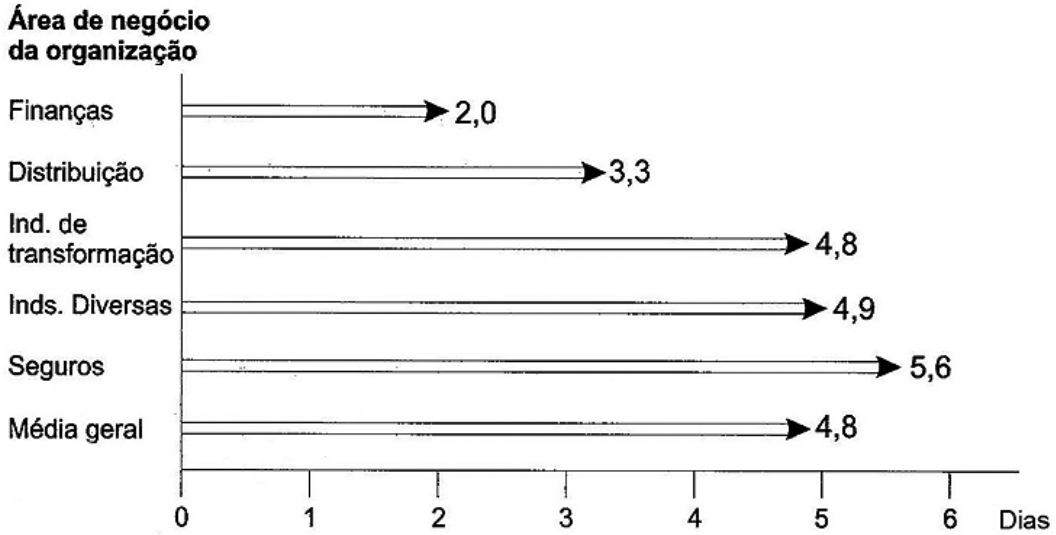
1 INTRODUÇÃO

Primariamente, o plano de contingência e de recuperação de desastres significa 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 fiquem parados acarrete perdas materiais aos negócios da empresa (IMONIANA, 2011).

De acordo com Sêmola (2003, p. 103), "os planos de contingência são desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencente ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência".

> O plano de contingência consiste em procedimentos de recuperação preestabelecidos, com a finalidade de minimizar o impacto sobre as atividades da organização no caso de ocorrência de um dano ou desastre que os procedimentos de segurança não conseguiram evitar. (CARUSO; STEFFEN, 1999, p. 289).

FIGURA 21 – PERÍODO TEMPO DURANTE O QUAL FUNÇÕES ESSENCIAIS SE MANTÊM APÓS UM DESASTRE



FONTE: Caruso e Steffen (1999, p. 290)

De acordo com Caruso e Steffen (1999, p. 289), as atividades de uma organização entram rapidamente em colapso após um desastre no seu ambiente de processamento de informações (figura anterior). O objetivo de um plano de contingência é servir como guia para esquematizar a execução de ações a ser tomadas para a continuidade dos serviços essenciais das áreas de negócios que dependam de um computador.

Para minimizar os esforços, reduzir os custos e tornar um plano de contingência factível e exequível, somente os serviços essenciais para dar continuidade aos negócios da organização devem ser contemplados no mesmo.

Entretanto, cada área de negócio da organização será responsável por definir o que é considerado serviço essencial, levando em conta o grau de criticidade do sistema avaliado para os negócios da organização.

FONTE: Caruso e Steffen (1999, p. 289)

O plano de continuidade, como é conhecido, numa visão secundária é muito mais que somente recuperação das atividades de informática. Contempla também as preocupações concernentes à vida dos funcionários, impacto sobre o meio ambiente, imagens junto aos clientes e fornecedores e o público em geral (IMONIANA, 2011).

Conforme Imoniana (2011, p. 167), "a responsabilidade básica é da diretoria da área de Tecnologia de Informações, se o ambiente for muito complexo. Se o ambiente for moderado, é do gerente de tecnologia de informações, e se for ambiente pequeno, é do encarregado ou dos analistas de sistemas responsáveis pela administração da rede". No entanto, para que sejam efetivas, a alta direção precisa dar apoio às medidas, visto que têm intuito estratégico.

Ao implementá-lo efetivamente, Imoniana (2011) comenta que se devem estabelecer os responsáveis pela consecução das ações de contingência, normalmente as pessoas designadas a assumir ações de contingências no momento de desastres são pessoas diferentes daquelas que executam funções operacionais no dia a dia em ambiente de tecnologia de informações. Para evitar conflitos, as responsabilidades são delineadas e 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 transformação dos mesmos sem causar descontinuidade operacional da empresa, em caso da quebra de equipamentos ou ocorrência de algum sinistro.

No processo de implementação do plano de contingência, recomenda-se que o usuário avalie-se 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 classificadas a seguir:

A – Alto risco
B – Risco intermediário
C – Baixo risco

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

FONTE: Imoniana (2011, p. 168)

A avaliação dos planos de contingência de uma empresa, de acordo com Imoniana (2011, p. 168), são certificar-se de que:

- Há planos desenvolvidos que contemplem todas as necessidades de contingências.
- Esses planos são suficientemente abrangentes para cobrir aspectos físicos, lógicos, de redes, de propriedades intelectuais, de pessoas, transacionais, entre outros.
- A equipe de contingência está preparada para as eventualidades.
- Esses planos são testados periodicamente.
- Os *backups* são atualizados.
- Os mesmos *backups* podem ser recuperados com pouca ou nenhuma dificuldade.
- Há relatórios gerenciais que facilitam o acompanhamento dos procedimentos.
- Os relatórios são confiáveis.

Para fins de familiarização, Imoniana (2011) cita que serão abordados, neste plano, somente casos com níveis de riscos altos e/ou intermediários em ambiente de rede operada pelas empresas médias.

Para fins desse plano, segundo Imoniana (2011, p. 169), geralmente as empresas industriais costumam estabelecer as seguintes aplicações mais críticas das empresas:

- Sistemas de Faturamento/Contas a Receber.
- Sistemas de Compras/Contas a Pagar.
- Sistemas de Recursos Humanos/Folha de Pagamento.
- Sistemas de Estoques/Custo de Produção.
- Sistema de Contabilidade Geral.

2 ANÁLISE DE RISCOS POTENCIAIS

O ambiente em análise, uma vez classificado como médio no uso de tecnologia de informações, opera redes de computadores com pouca complexidade. A seguir, Imoniana

(2011, p. 169-170) aborda os riscos potenciais:

QUADRO 13 – RISCOS DE TECNOLOGIA DE INFORMAÇÃO

Riscos de Tecnologia de Informação	Alto	Médio	Baixo
Switch – Equipamento responsável por orientar o tráfego de pacotes (informações na rede). Conversor ATM/ETHERNET – Equipamento que tem a função de *Switch* e conversor de pacotes.	X		
ATM/ETHERNET – Tipos de redes de computadores. Servidores. Servidores Área Industrial. CPD. Sala de Operação.	X		
Backbone – Meio físico principal de uma rede (cabeamento). *Roteador* – Equipamento que define rotas para os pacotes numa rede. *Hub* – Equipamento que faz a conexão da placa de rede do computador e da rede. Linhas telefônicas.		X	
SWITCH ATM – Equipamento responsável pela interligação dos servidores e a rede da área industrial com a rede da área administrativa.	X		
Conversor ATM/ETHERNET – Equipamento responsável pela conversão de pacotes ATM em Ethernet e vice-versa, além de interligar todos os *backbones* departamentais.	X		
Servidores gerenciadores de recursos compartilhados.	X		
Servidores da área industrial – servidores pouco usados.			X
Equipamentos de centro de processamento de dados.	X		
Equipamentos para gerenciamento de operações.		X	
Backbones corporativos, administrativos e operacionais.		X	
Equipamentos e periféricos da rede.	X		
Sistemas aplicativos: • Sistema de Faturamento/Contas a Receber. • Sistema de Compras/Contas a Pagar. • Sistema de Recursos Humanos/Folha de Pagamento. • Sistema de Estoque/Custo de Produção. • Sistema de Contabilidade Geral.	 X X X	 X	 X

FONTE: Adaptado de Imoniana (2011, p. 169-170)

3 CONTINGÊNCIA EM RELAÇÃO AOS RECURSOS TECNOLÓGICOS

Um plano de contingência não precisa necessariamente utilizar equipamentos similares aos envolvidos no evento gerador da contingência. Como um plano de contingência é um caminho alternativo para dar continuidade aos negócios da organização, deve-se

> escolher qualquer recurso disponível, que pode ser: manual, utilização de microcomputadores ou até mesmo outro computador de grande porte. O fato que determinará esse caminho será o que envolver menor custo, facilidade de acesso, utilização e disponibilidade de recursos computacionais. (CARUSO; STEFFEN, 1999, p. 291).

Para este caso específico, havendo indisponibilidade, segundo Imoniana (2011, p. 170), "existe um contrato de manutenção, no qual a empresa contratada responsabiliza-se em colocar outro equipamento semelhante, dento de um prazo de tempo mínimo, no qual a inatividade operacional da empresa não passe a interferir em seu funcionamento". A rede da área industrial continuará a operar normalmente, pois ela já possui sua própria redundância, ficando somente prejudicada a sua interligação com o servidor de banco de dados, o que não interfere na sua continuidade operacional.

No que diz respeito aos servidores, de acordo com Imoniana (2011, p. 170-171),

> no caso da indisponibilidade de um dos componentes (periféricos) acessórios dos servidores (memória, placa *Disk array*, discos magnéticos, unidades de fita DAT), existirá sempre um reserva (*backup*) deste, que deverá ser utilizada. Caso a indisponibilidade seja em relação a CPU/ fonte do servidor, deverá ser utilizado um servidor reserva (caso exista), se não, será desativado temporariamente e em último caso haverá a utilização de um servidor da área industrial.

Os servidores da área industrial são sempre redundantes, pois em caso de falha de algum, o outro assume automaticamente. No caso da perda de todos os servidores, serão utilizados micros comuns e quantos forem necessários, conforme especificação da área industrial (IMONIANA, 2011).

No caso de indisponibilidade total do CPD (servidores/*switch* e equipamentos de rede), conforme Imoniana (2011, p. 171), deverão ser tomadas as seguintes medidas para manter a continuidade operacional da empresa:

a) Utilização de servidores da área industrial conforme negociado.
b) Capacitação dos servidores nos requerimentos mínimos de *hardware*, conforme o tipo de servidor (rede e banco de dados).
c) Substituição dos *switches* ATM por Ethernet.
d) Manutenção da estrutura da 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.

Em caso de indisponibilidade total da sala de operação, Imoniana (2011) recomenda que deverão ser utilizados micros comuns no lugar dos servidores, e em relação às placas da SMAR, será seguido o plano de contingência da área industrial/instrumentação.

De acordo com Imoniana (2011, p. 171), "no caso da indisponibilidade do *backbone* corporativo, o *switch* ATM deverá ser transferido para a sala do CPD, e utilizados cordões ópticos para restabelecer suas interligações".

Na eventual indisponibilidade do *backbone* departamental, conforme Imoniana (2011, p. 171), "os usuários deverão utilizar os equipamentos em alguma outra área não afetada".

Caso ocorra a indisponibilidade de todos os *backbones*, Imoniana (2011, p. 172) recomenda que seja instalado um mini-CPD na área de informática com os seguintes procedimentos:

a) Utilização de um Hub Ethernet como módulo central.
b) Conversão dos servidores da ATM para Ethernet.
c) Alteração do sistema de balança para entrada manual.
d) Disponibilização dos micros da informática para uso das principais necessidades da empresa.

4 CONTINGÊNCIAS EM RELAÇÃO A APLICATIVOS CRÍTICOS

No caso da indisponibilidade das linhas telefônicas por períodos prolongados e não suportados, segundo Imoniana (2011, p. 172-173), deverão ser tomadas as seguintes medidas em relação aos sistemas:

Sistemas de faturamento/contas a receber
i) Emissão das Notas Fiscais em São Caetano do Sul; ou
ii) Emissão manual de Notas Fiscais.
iii) Utilização do *hot-site* já contratado.

Sistemas de compras/contas a pagar
i) Solicitações de compras e pagamentos feitos manualmente; ou
ii) Utilização do *hot-site* já contratado.

Sistemas de contabilidade geral
i) Os lançamentos deverão ser feitos no *hot-site* já contratado.
ii) Utilização do centro de processamento de dados de São Caetano do Sul.

Sistema de recursos humanos/folha de pagamento
i) Utilização do centro de processamento de dados de São Caetano do Sul; ou
ii) Utilização de *hot-site* se for necessário.

5 MATRIZ DE RESPONSABILIDADES

A seguir, Imoniana (2011, p. 173) apresenta a matriz de responsabilidades da equipe de contingência.

QUADRO 14 – MATRIZ DE RESPONSABILIDADE DA EQUIPE DE CONTINGÊNCIA

Nome	Responsabilidade	Autoridade Delegada	Telefones de contato
Joaquim Nabuco	Controle da rede	Analista de sistemas da área de informática	4457-8970
Joshua Imoniana	Controle de dados	Gerente de auditoria de sistemas	5868-9999
Bernardete Bezerra	Controle de processamentos	Supervisão das operações	6768-4656
Washington Junior	Localização e uso de *backups*	Supervisor de segurança	3446-5678
Martha Silva	Contatos e ativação de *hot-site*	Gerente de informática	2436-5567
Anthony Santana	Controles de procedimentos de contingência, registro de exceções e dos custos	Auditor de sistemas sênior	3446-4547
José Silva	Controles de documentos do processo de contingência	Supervisor de logística	3454-4654
Carlos Luiz	Transportes e relocação de pessoas	Administrador de *help-desk*	3454-4549
Carolina Silva	Monitoramento e relatório de contingência	Administrador de banco de dados	3434-3445

FONTE: Adaptado de Imoniana (2011, p. 173)

6 AVALIAÇÃO DO PLANO DE CONTINGÊNCIA

Schmidt, Santos e Arima (2006, p. 47-48) recomendam que, sob a ótica da auditoria, devem ser observados os seguintes aspectos:

- Identificação do pessoal responsável e predeterminado para aplicação do plano de contingência.
- Comunicação aos responsáveis pelo plano de contingência com referência a alterações que comprometam a utilização do site alternativo.
- Existência de provisões de facilidades de reserva de tecnologia da informação com outros usuários em caso de quebra ou instabilidade de equipamentos correspondentes.
- Compatibilidade de sistemas operacionais ou *softwares* com as instalações de outros usuários.
- Clareza nas prioridades de ativação das funções dos sistemas de informações em caso de sinistro.
- Verificação da adequação de rotinas para reconstrução de arquivos magnéticos.
- Explicação detalhada para a correção e restauração do ambiente de tecnologia da informação, em termos de *hardware* e *software*.
- Revisão e teste regular e periódico do plano de contingência.

O quadro a seguir demonstra um programa de teste de controles para avaliação do plano de contingência.

QUADRO 15 – *CHECK-LIST* PARA AUDITORIA DE PLANO DE CONTINGÊNCIA

		***Check-list* para auditoria de plano de contingência**	SIM	NÃO
C1 – Planejamento Estratégico de Continuidade inclusive:				
		a) Referência à documentação comprobatória contemplando cronograma geral. b) Indicação de atividades, prazos e responsáveis. c) Identificação dos processos operacionais críticos da instituição, bem como das evidências do envolvimento da alta administração nesse processo. d) Mapeamento (matriz de impacto) utilizado no desenvolvimento dos planos de contingência. e) Relação dos processos operacionais críticos, identificados nos itens anteriores, e dos recursos de *hardware*, *software* e infraestrutura (redes, telefonia, energia elétrica etc.) que os suportam. f) Planos de testes periódicos para constatar sua funcionalidade.		
	P1 –	O plano de continuidade é concebido com aval da alta administração? Se sim, descreva o processo de aprovação.		
	P2 –	Identificar os processos e aplicações críticas da empresa que seriam mais afetados em caso de paralisação na área de informática e comparar com os identificados no plano de continuidade.		
	P3 –	Documentar a consistência dos procedimentos a serem adotados para os diferentes graus e extensão de desastre.		

C2 – Análise de Riscos Potenciais e das Probabilidades de Ocorrência de Falhas nos diferentes recursos do parque de informática da instituição: *hardware*, *software* e infraestrutura, baseada na avaliação da administração, quanto ao grau de dependência que esses recursos possuam em relação ao processamento de dados.				
	P1 –	Informar entre 0 e 1,0 o grau aparente de vulnerabilidade do ambiente em caso de interrupções dos processos operacionais críticos da entidade.		
	P2 –	Comparar o grau aparente com aquele constatado na avaliação anterior do ambiente de processamento de dados.		
C3 – Seleção de estratégias de continuidade adotadas pela administração para cada processo de contingência, tais como: utilização de recursos de informática e de infraestrutura alternativos, tempos de ativação exigidos, serviços possíveis de serem disponibilizados, custos envolvidos etc. e procedimentos para revisão sistemática dos planos.				
	P1 –	Constar a base para a seleção das estratégias escolhidas pela alta administração.		
	P2 –	Evidenciar a razoabilidade da decisão tomada na escolha das infraestruturas alternativas.		
	P3 –	Constar a razoabilidade do tempo de ativação das operações normais do *hot-site*.		
	P4 –	Analisar a relação custo/benefícios do *hot-site* em relação aos outros, se existirem.		
	P5 –	Verificar a documentação e ou registro da revisão sistêmica dos planos, atentando para sua efetividade.		

C4 – Testes preventivos do funcionamento do plano de contingência e de recuperação de dados.				
	P1 –	Verificar a conscientização sobre os procedimentos e as responsabilidades para recuperação de dados, programas, *software* e documentação quanto: • Quem faz o quê. • Necessidades de comunicação de dados. • Facilidade administrativa. • Localização e maneira de obtenção do material de *backup*. • Transporte dos arquivos, manuais etc. • Procedimentos para utilização de outras instalações (CPD, *backup*, contratos com *bureau* de serviços, contratos com empresas próximas de mesmo porte). • Realocação de pessoal.		
C5 – Aprovação formal dos planos de contingência pelo diretor responsável e pelo comitê de contingência				
	P1 –	Verifique a existência de procedimentos documentados para a aprovação do plano de contingência e de recuperação de desastres.		
	P2 –	O responsável geral pela implementação de contingência também dá OK ao processo de aprovação?		
	P3 –	Os líderes de contingência, que não necessariamente precisam ser os analistas de sistemas, recebem os planos aprovados?		
	P4 –	A equipe toda recebe cópias dos planos devidamente aprovados?		
	P5 –	Se sim, solicite que um integrante da equipe de contingência mostre sua cópia aprovada.		

7 APROVAÇÃO FORMAL DO PLANO DE CONTINGÊNCIA

Como instrumento de oficialização dos interesses da empresa em adequar o nível de segurança de suas informações a partir do envolvimento de todos os níveis hierárquicos é conveniente que o presidente, CEO ou CIO externe esta vontade oficialmente. A Carta do Presidente tem esse papel e é disponibilizada, quando não, encaminhada a cada funcionário, dando um caráter formal ao movimento. Por vezes, este documento aparentemente simples, é responsável por muitos apoios espontâneos e o natural fortalecimento do plano estratégico de segurança da informação (SÊMOLA, 2003).

RESUMO DO TÓPICO 2

Caro(a) acadêmico(a)! Neste tópico, você estudou que:

- O plano de contingência consiste em procedimentos de recuperação preestabelecidos, com a finalidade de minimizar o impacto sobre as atividades da organização no caso de ocorrência de um dano ou desastre que os procedimentos de segurança não conseguiram evitar.

- O objetivo de um plano de contingência é servir como guia para esquematizar a execução de ações a ser tomadas para a continuidade dos serviços essenciais das áreas de negócios que dependam de um computador.

- Cada área de negócio da organização será responsável por definir o que é considerado serviço essencial, levando em conta o grau de criticidade do sistema avaliado para os negócios da organização.

- Após a avaliação do nível de risco, o usuário deve verificar que tipo de proteção é a mais recomendada.

- O ambiente em análise, uma vez classificado como de risco médio no uso de tecnologias da informação opera redes de computadores com pouca complexidade.

- Como um plano de contingência é um caminho alternativo para dar continuidade aos negócios da organização, deve-se escolher qualquer recurso disponível, que pode ser: manual, utilização de microcomputadores ou até mesmo outro computador de grande porte.

- Por vezes, a carta do presidente da empresa é responsável por muitos apoios espontâneos e o natural fortalecimento do plano estratégico de segurança da informação.

AUTOATIVIDADE

1 Cite três avaliações dos planos de contingência de uma empresa.

2 Cite três medidas que devem ser tomadas para manter a continuidade operacional da empresa.

3 Monte uma matriz de responsabilidade da equipe de contingência da empresa na qual você trabalha.

4 Cite alguns os aspectos que devem ser observados sob a ótica da auditoria referentes à avaliação do plano de contingência.

5 Elabore um *check-list* para auditoria de plano de contingência que pode ser aplicado na sua empresa.

Assista ao vídeo de resolução da questão 3

TÓPICO 3

POLÍTICA DE SEGURANÇA

1 INTRODUÇÃO

Na vida das pessoas e das organizações, tudo gira em termos de decisões políticas, não importando quem tome essas decisões e que nome seja dado. Qualquer organização sempre estabelece regulamentos políticos a serem seguidos por todos quantos se relacionem com ela. Exemplos de políticas são os estatutos sociais das empresas, clubes e outras organizações, descrições de procedimentos técnicos e outros.

Não há como negar; tudo na vida é política; é o que mais fazemos: discutir sobre política. Portanto, vamos discutir sobre a política de segurança que uma organização deve implementar para proteger seus ativos.

FONTE: Caruso e Steffen (1999, p. 49)

A alta administração da organização emitiu uma política de segurança da informação ativa e abrangente? Essa política é sujeita a revisões periódicas e a atualizações quando necessário?

Todos os usuários de informações e sistemas de informações na organização precisam conhecer seus papeis e responsabilidades para proteger os ativos da empresa. A política de segurança da informação visa comunicar e estabelecer essa responsabilidade de cada um para com a confidencialidade, integridade e disponibilidade das informações. A política estabelece os objetivos e expectativas com relação ao tratamento a serem dados por cada integrante na organização às informações, seus controles e padrões e procedimentos estabelecidos. O seu texto deve ser claro e direto o suficiente para que cada um na organização o entenda e não restem dúvidas sobre o seu conteúdo e sua interpretação. A política também deve estabelecer e trazer descrito as sanções pelo seu não cumprimento. Como a política é estabelecida pela alta administração da organização, e não pelo seu *Security Officer*, é importante que o seu texto seja executivo, genérico, duradouro em termos de ser ligado aos conceitos da informação e administração, e não à tecnologia ou a aspectos momentâneos da organização. Os detalhes e descrições a respeito do cumprimento da política estarão em outros documentos subordinados em hierarquia à política, e esses sim, definidos pelo *Security Officer*. Em geral, a

política é a cabeça da pirâmide da função segurança da informação, sustentada por padrões e procedimentos. O *Security Officer* auxilia estrategicamente na definição e manutenção da política, mas que a assina e exige cumprimento é o Presidente ou o principal executivo da organização.

FONTE: Ferreira e Araújo (2008, p. 187)

A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações. A necessidade de estabelecer uma política de segurança é um fato realçado unanimemente em recomendações tanto do meio militar (como o *Orange Book* do Departamento de Defesa dos Estados Unidos) como no meio técnico (como o *Site Security Handbook [Request for Comments* – RFC] 2196 do *Institute Engineering Task Force* e, mais recentemente, do meio empresarial (norma *International Standartization Organization/International Electricaltechnical Comission* (ISO/IEC) 17799) (NAKAMURA; GEUS, 2007). Obs.: A norma ISO/IEC 17799 foi atualizada para a numeração ISO/IEC 27002 em julho de 2007.

> Seu desenvolvimento é o primeiro e principal passo da estratégia de segurança das organizações. É por meio dessa política que todos os aspectos envolvidos na proteção dos recursos existentes são definidos e, portanto, grande parte do trabalho é dedicada à sua elaboração e ao seu planejamento. No entanto, veremos que as maiores dificuldades estão mais na sua implementação do que em seu planejamento e elaboração. (NAKAMURA; GEUS, 2007, p. 188).

Assim, a política de segurança trata dos aspectos humanos, culturais e tecnológicos de uma organização, levando também em consideração os processos e os negócios, além da legislação local. É com base nessa política de segurança que as diversas normas e os vários procedimentos devem ser criados.

Além de seu papel primordial nas questões relacionadas com a segurança, a política de segurança, uma vez fazendo parte da cultura da empresa, tem uma importante função como facilitadora e simplificadora do gerenciamento de todos os seus recursos. De fato, o gerenciamento de segurança é a arte de criar e administrar a política de segurança, pois não é possível gerenciar o que não pode ser definido.

FONTE: Nakamura e Geus (2007, p. 189)

2 CONSIDERAÇÕES IMPORTANTES

Com o propósito de fornecer orientação e apoio às ações de gestão de segurança, a política tem um papel fundamental e, guardadas as devidas proporções, tem importância similar à constituição federal para um país. Desta forma, assume uma grande abrangência e, por conta disso, é subdividida em três blocos: diretrizes, normas, procedimentos e instruções, sendo destinados, respectivamente, às camadas estratégica, tática e operacional.

Estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa; portanto, a política deve ser personalizada.

As diretrizes, que por si só, têm papel estratégico, precisam expressar a importância que a empresa dá para a informação, além de comunicar aos funcionários seus valores e seu comprometimento em incrementar a segurança à sua cultura organizacional.

É notória a necessidade do envolvimento da alta direção, refletida pelo caráter oficial com que a política é comunicada e compartilhada com os funcionários. Este instrumento deve expressar as preocupações dos executivos e definir as linhas de ação que orientarão as atividades táticas e operacionais.

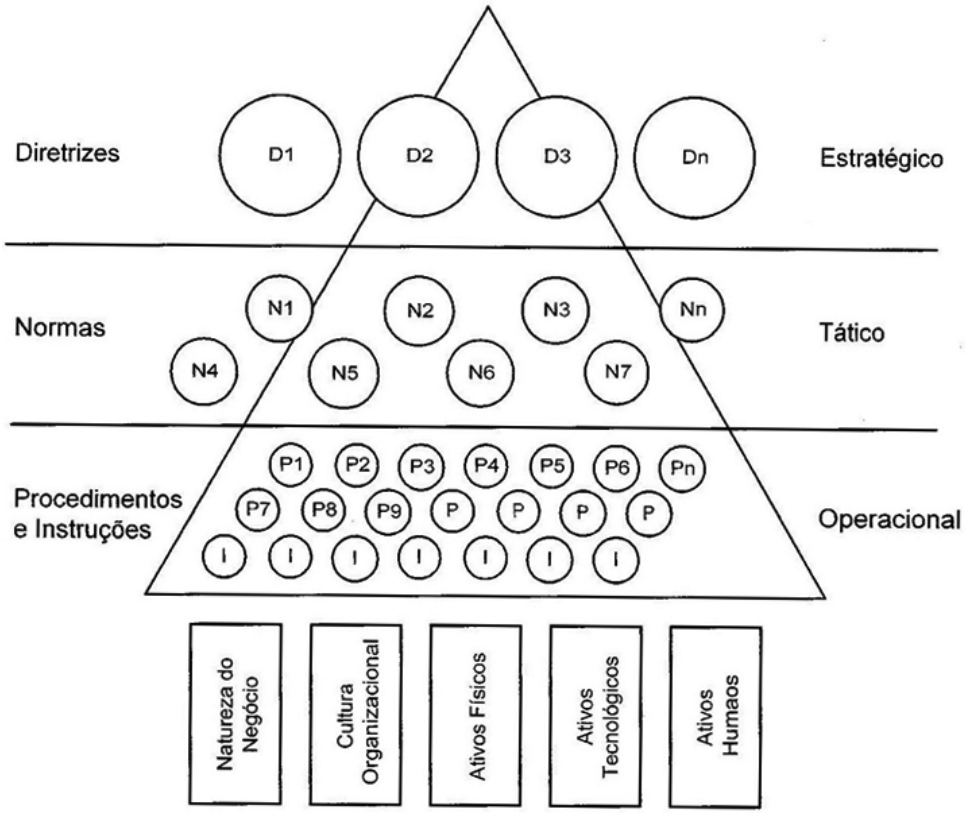
Responsabilidades dos proprietários e custodiantes das informações, estrutura do *Security Office*, métricas, índices e indicadores do nível de segurança, controles de conformidade legal, requisitos de educação e capacitação de usuários, mecanismos de controle de acesso físico e lógico, responsabilizações, auditoria do uso de recursos, registros de incidentes e gestão da continuidade do negócio são algumas das dimensões a serem tratadas pela política de segurança.

FONTE: Sêmola (2003, p. 105)

Marcos Sêmola (2003, p. 105-106) relata que,

> com caráter tático, as normas são o segundo nível da política. Detalham situações, ambientes, processos específicos e fornecendo orientação para o uso adequado das informações. Baseado em ordem de grandeza, podemos estimar 10 a 20 diretrizes em empresas de qualquer porte, mas temos de multiplicar este número por 100 ou mais para estimar o volume de normas aplicáveis. Este volume tende a ser proporcional ao porte da empresa, à heterogeneidade de seus ativos físicos, tecnológicos e humanos e, ainda, ao grau de detalhamento necessário para levar a empresa a operar sob o nível de risco adequado.

FIGURA 22 – DIAGRAMA DOS COMPONENTES DA POLÍTICA E SEUS PILARES DE SUSTENTAÇÃO



FONTE: Sêmola (2003, p. 106)

Critérios normatizados para admissão e demissão de funcionários; criação e manutenção de senhas; descarte de informação em mídia magnética; desenvolvimento e manutenção de sistemas; uso da internet; acesso remoto; uso de *notebook*; contratação de serviços de terceirizados; e classificação da informação, são bons exemplos de normas de uma típica política de segurança (SÊMOLA, 2003).

> Em especial, a norma de classificação da informação é fator crítico de sucesso, pois assume a responsabilidade por descrever os critérios necessários para sinalizar a importância e o valor das informações, premissa importante para a elaboração de praticamente todas as demais normas. Não há regra preconcebida para estabelecer esta classificação; mas é preciso entender o perfil do negócio e as características das informações que alimentam os processos e circulam no ambiente corporativo para que os critérios sejam personalizados. (SÊMOLA, 2003, p. 106-107).

FIGURA 23 – RELAÇÃO ENTRE CLASSIFICAÇÃO E TRATAMENTO DEFINIDO NA POLÍTICA

FONTE: Sêmola (2003, p. 107)

Procedimentos e instruções deverão estar presentes na política em maior quantidade por seu perfil operacional, onde é necessário descrever meticulosamente cada ação e atividade associada a cada situação distinta de uso das informações. Por exemplo: enquanto a diretriz orienta estrategicamente para a necessidade de salvaguardar as informações classificadas como confidenciais, e a norma define que estas deverão ser criptografadas em tempo de envio por *e-mail*, o procedimento e a instrução específica para esta ação têm de descrever os passos necessários para executar a criptografia e enviar o *e-mail*. A natureza detalhista deste componente da política pressupõe a necessidade de manutenção ainda mais frequente (SÊMOLA, 2003).

Diante disso, já é possível perceber o quão complexo é desenvolver e, principalmente, manter atualizada a política de segurança da informação com todos os seus componentes. Esta percepção torna-se ainda mais latente ao considerarmos o dinamismo do parque tecnológico de uma empresa e, ainda, as mudanças previsíveis e imprevisíveis que o negócio poderá sofrer. Dessa forma, o importante é dar o pontapé inicial e formar um grupo de trabalho com representantes das áreas e departamentos mais representativos, integrando visões, percepções e necessidades múltiplas que tenderão a convergir e gerar

os instrumentos da política. Comece elaborando as diretrizes, envolva os executivos e conquiste apoio. Estabeleça os responsáveis e os gestores diretos da manutenção da política. Desenvolva um programa de divulgação das diretrizes, normas, procedimentos e instruções da política como instrumento para disseminação de cultura e conscientização dos funcionários. Lance mão de seminários, cartazes, brindes, comunicações oficiais dos executivos, cursos convencionais ou *on-line*, protetores de tela e tudo mais que se aplicar ao perfil da empresa e à natureza de sua atividade. O importante é envolver todos os funcionários, fazendo-os se sentir corresponsáveis pela saúde da segurança do negócio e, principalmente, responsáveis pela proteção das informações por eles custodiadas.

FONTE: Sêmola (2003, p. 107-108)

"A conformidade com requisitos legais, envolvendo obrigações contratuais, direitos de propriedade intelectual, direitos autorais de *software* e todas as possíveis regulamentações que incidam no negócio da empresa devem ser respeitados e, portanto, deve ser a linha de conduta da construção da política de segurança". (SÊMOLA, 2003, p. 108).

> Para assegurar que a política de segurança da informação esteja sempre aplicável à realidade da organização e continue relevante para a proteção dos ativos de informação é importante a sua revisão periódica. Recomenda-se que anualmente seja feita uma revisão e atualização no seu texto, se aplicável. As boas práticas de segurança da informação também estabelecem juntamente com a política de segurança da informação um termo de responsabilidade a ser assinado pelos usuários de informação e facilidades de sistemas e processos na organização. (FERREIRA; ARAÚJO, 2008, p. 187).

"As empresas necessitam de segurança das informações, pois todos os dias novos usuários estão tentando descobrir novos furos de segurança, seja de forma intencional ou por acidentes, pois cada dia estamos mais dependentes dos sistemas de informação". (MONTEIRO, 2003, p. 134).

Conforme Nakamura e Geus (2007, p. 219),

> a política de segurança é o principal elemento para a segurança de qualquer empresa. Seu planejamento e definição dos aspectos a serem tratados incluem uma avaliação de todos os detalhes envolvidos, o que requer o esforço de todos na organização. Diversos obstáculos para a sua implementação são resultantes da visão errada que a segurança não é um elemento importante para a organização, o que, invariavelmente,

> traz sérias consequências com a invasão dos *hackers*. Alguns pontos específicos requerem uma política específica, como no caso do acesso remoto, do uso das senhas e do *firewall*. A política de segurança tem uma importância ainda maior em um ambiente cooperativo, no qual os bolsões de segurança variam de tamanho, de acordo com as necessidades de conexão.

3 PLANEJAMENTO DA POLÍTICA

O início do planejamento da política de segurança exige uma visão abrangente, de modo que os riscos sejam entendidos para que possam ser enfrentados. Normalmente, a abordagem com relação à segurança é reativa, o que pode, invariavelmente, trazer futuros problemas para a organização. A abordagem proativa é, portanto, essencial e depende de uma política de segurança bem definida, na qual a definição das responsabilidades individuais deve estar bem clara, de modo a facilitar o gerenciamento da segurança em toda a organização (NAKAMURA; GEUS, 2007).

De acordo com Nakamura e Geus (2007, p. 189), "ter uma política proativa também é fundamental, pois, sem essa abordagem, a questão da segurança das informações não é 'se', mas sim 'quando' o sistema será atacado por um *hacker*".

> O apoio dos executivos é importante para que isso aconteça, o que faz com que os recursos financeiros para as soluções necessárias sejam garantidos. Quando uma política de segurança é planejada e definida, os executivos demonstram claramente o seu comprometimento e apoio à segurança da informação de toda a organização. Um ponto importante para que a política tenha o seu devido peso dentro da organização é que ela seja aprovada pelos executivos, publicada e comunicada para todos os funcionários, de forma relevante e acessível. (NAKAMURA; GEUS, 2007, p. 189-190).

O planejamento da política de segurança deve ser feito tendo como diretriz o caráter geral e abrangente de todos os pontos, incluindo as regras que devem ser obedecidas por todos. Essas regras devem especificar quem pode acessar quais recursos, quais são os tipos de usos permitidos no sistema, bem como os procedimentos e controles necessários para proteger as informações.

Uma visão geral do planejamento pode ser observada na figura a seguir, na qual a pirâmide mostra que a política fica no topo, acima das normas e procedimentos. A política é o elemento que orienta as ações e as implementações futuras, de uma maneira global, enquanto as normas abordam os detalhes, como os passos da implementação, os conceitos e os projetos de sistemas e controles. Os procedimentos são utilizados para que os usuários possam cumprir aquilo que foi definido na política e os administradores de sistemas possam configurar os sistemas de acordo com a necessidade da organização.

FONTE: Nakamura e Geus (2007, p. 190)

FIGURA 24 – O PLANEJAMENTO DA POLÍTICA DE SEGURANÇA

FONTE: Nakamura e Geus (2007, p. 190)

A política de segurança pode também ser dividida em vários níveis, partindo de um nível mais genérico (para que os executivos possam entender o que está sendo definido), passando pelo nível dos usuários (para que eles tenham consciência de seus papéis para a manutenção da segurança na organização) chegando ao nível técnico (que se refere aos procedimentos específicos, como a definição e a implementação das regras de filtragem do *firewall*) (NAKAMURA; GEUS, 2007).

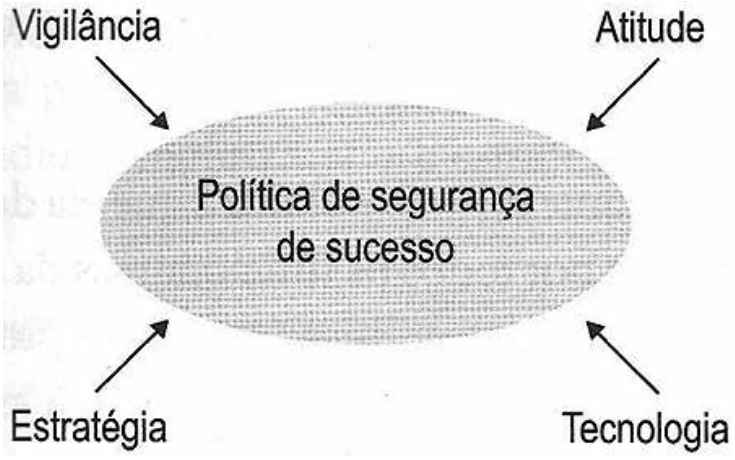
4 ELEMENTOS DA POLÍTICA DE SEGURANÇA

Os elementos que uma política de segurança adequada deve possuir, de acordo com Nakamura e Geus (2007, p. 191), tudo aquilo que é essencial para o combate às adversidades. O que deve ser mantido não é apenas a proteção contra os ataques de *hackers*, mas também a disponibilidade da infraestrutura da organização. Esses elementos essenciais para a definição da política de segurança e para sua implantação são:

- Vigilância: significa que todos os membros da organização devem entender a importância da segurança para a mesma, fazendo com que atuem como guardiões da rede, evitando-se, assim, abusos sistêmicos e acidentais.
- Atitude: significa a postura e a conduta quanto à segurança. Sem a atitude necessária, a segurança proposta não terá nenhum valor.
- Estratégia: diz respeito a ser criativo quanto às definições da política e do plano de defesa contra intrusões, além de possuir a habilidade de ser adaptativo a mudanças no ambiente, tão comuns no meio cooperativo.
- Tecnologia: a solução tecnológica deve ser adaptativa e flexível, a fim de suprir as necessidades estratégicas da organização, pois qualquer tecnologia um pouco inferior resulta em um falso e perigoso senso de segurança, colocando em risco toda a organização.

Assim, a vigilância, atitude, estratégia e tecnologia (figura a seguir) podem ser consideradas os fatores de sucesso da política de segurança.

FIGURA 25 – FATORES DE SUCESSO DA POLÍTICA DE SEGURANÇA



FONTE: Nakamura e Geus (2007, p. 193)

Segundo Nakamura e Geus (2007, p. 193), "a política de segurança não deve conter detalhes técnicos específicos de mecanismos a serem utilizados ou procedimentos que devem ser adotados por indivíduos particulares, mas, sim, regras gerais e estruturais que se aplicam ao contexto de toda a organização". Com isso, "a política pode ser flexível o suficiente para que não sofra alterações frequentes". Além disso, "ela pode ser abrangente o bastante para abarcar possíveis exceções". (NAKAMURA; GEUS, 2007, p. 193-194).

> Uma característica importante de uma política é que ela deve ser curta o suficiente para que seja lida e conhecida por todos os funcionários da empresa. A essa política de alto nível devem ser acrescentados políticas, normas e procedimentos específicos para setores e áreas particulares, como por exemplo, para a área de informática. (NAKAMURA; GEUS, 2007, p. 194).

5 CONSIDERAÇÕES SOBRE A SEGURANÇA

Conforme Nakamura e Geus (2007, p. 194), "antes de desenvolver a política de segurança, é necessário que os responsáveis pela sua criação tenham o conhecimento dos diversos aspectos de segurança, além da familiarização com as questões culturais, sociais e pessoais que envolvem o bom funcionamento da organização".

Ainda segundo Nakamura e Geus (2007, p. 194), algumas considerações sobre a segurança, importantes para a definição de uma boa política de segurança, são:

- Conheça seus possíveis inimigos: identifique o que eles desejam fazer e os perigos que eles representam à sua organização.

- Contabilize os valores: os custos das medidas de segurança devem ser compatíveis e proporcionais às necessidades da organização e às probabilidades de ocorrerem incidentes de segurança.
- Identifique, examine e justifique suas hipóteses: qualquer hipótese esquecida ou não divulgada pode causar sérios problemas de segurança. Uma única variável pode mudar completamente a estratégia de segurança de uma organização.
- Controle seus segredos: muitos aspectos de segurança têm como base os segredos, que devem ser guardados 'a sete chaves'.
- Avalie os serviços estritamente necessários para o andamento dos negócios da organização: a segurança é inversamente proporcional às funcionalidades e pode influir na produtividade dos usuários. Determinar e justificar cada serviço permitido é essencial para evitar conflitos futuros com os usuários.
- Considere os fatores humanos: muitos procedimentos de segurança falham, pois, não se consideram as reações dos usuários a esses procedimentos. Cada usuário deve ser convencido da necessidade de cada medida a ser adotada. Eles devem entender e aceitar essas exigências de segurança. Minimiza a chance de sucesso de ataques que usam a engenharia social.
- Conheça seus pontos fracos: todo sistema tem suas vulnerabilidades. Conhecer e entender esses pontos fracos permite que o primeiro passo para proteger o sistema de maneira eficiente seja definido.
- Limite a abrangência do acesso: barreiras como uma zona desmilitarizada (DMZ) fazem com que, caso um sistema seja atacado, o restante da rede não seja comprometido. A parte segura de uma rede é tão 'forte' quanto a sua parte menos protegida.
- Entenda o ambiente: entender o funcionamento normal da rede é importante para detectar possíveis comportamentos estranhos, antes que um invasor cause prejuízos.
- Limite a confiança: é essencial estar atento e vigilante, principalmente quanto a programas de *software* que tenham muitos *bugs* e que podem comprometer a segurança do ambiente. Não se pode confiar totalmente em todos os sistemas e usuários da organização, e é preciso estar sempre atento a comportamentos anormais.
- Nunca se esqueça da segurança física: o acesso físico indevido a equipamentos ou roteadores pode destruir todas as medidas de segurança adotadas. O controle de acesso físico e o plano de contingência deve fazer parte da política de segurança da organização.
- A segurança é complexa: qualquer modificação em qualquer peça do ambiente pode causar efeitos inesperados no nível de segurança. Entender as implicações de segurança em cada aspecto envolvido é importante para a manipulação e o gerenciamento correto de todas as variáveis envolvidas.
- A segurança deve ser aplicada de acordo com os negócios da organização: entender os objetivos de negócios da organização é importante para a definição de sua estratégia de segurança.

Essas considerações, segundo Nakamura e Geus (2007, p. 196) "demonstram a importância de uma visão abrangente da segurança, o que torna o desafio da proteção dos negócios ainda maior".

6 PONTOS A SEREM TRATADOS PELA POLÍTICA DE SEGURANÇA

A política de segurança, definida de acordo com os objetivos de negócios da organização, deve existir de maneira formal, pois somente assim é possível implementar efetivamente a segurança. Caso isso não ocorra, os administradores da segurança devem documentar todos os aspectos a serem tratados, sendo imprescindível que a aprovação do executivo seja formalizada. Tal formalidade evitará que, no futuro, as responsabilidades recaiam totalmente sobre os administradores, além de impedir situações em que ocorram eventos que não são do conhecimento dos executivos e tragam consequências inesperadas e tensões desnecessárias à organização. Além do mais, a política de segurança formal é essencial, porque as responsabilidades quanto às questões de segurança, caso não estejam definidas na respectiva política, devem ser dos executivos, e não dos administradores de segurança.

FONTE: Nakamura e Geus (2007, p. 196-197)

De qualquer forma, é de responsabilidade dos administradores alertar sobre as questões de segurança e implementar as medidas definidas na política. Participar da definição dessa política, que envolve os aspectos de toda a organização, também é essencial, assim como determinar as normas e os procedimentos.

Sob a perspectiva do usuário, é essencial que exista sua participação no trabalho de desenvolvimento da política e também na definição das normas e procedimentos a serem adotados. Esse envolvimento é importante, porque medidas de segurança que atrapalham o usuário, invariavelmente, falham. As medidas devem ter a máxima transparência possível para o usuário, de modo que as necessidades de segurança da organização estejam em conformidade com suas próprias necessidades.

Assim, uma política de segurança adequada deve tratar não só dos aspectos técnicos, mas principalmente daqueles relacionados ao trabalho, às pessoas e ao gerenciamento. Ela deve abordar, especialmente, os aspectos do cotidiano, como, por exemplo, a definição dos cuidados necessários com documentos em mesas de trabalho e até mesmo com o lixo, pois esse é um dos locais mais explorados à procura de informações confidenciais.

Os aspectos culturais e locais também devem ser considerados na elaboração da política de segurança, pois eles influenciam diretamente na sua efetividade. A política de demissão de funcionários por falha na escolha de senhas, por exemplo, poderia ser aplicada nos Estados Unidos, mas na Europa o funcionário demitido poderia ganhar um processo na justiça. Essas

peculiaridades existentes em diferentes culturas fazem com que a ajuda de um profissional local, para o desenvolvimento ou a adequação da política de segurança da organização, seja um ponto importante a ser considerado.

A política de segurança deve definir também, do modo mais claro possível, as punições e os procedimentos a serem adotados, no caso do não cumprimento da política definida. Esse é um aspecto importante que precisa ser definido, para que os abusos sejam evitados e os usuários tenham consciência de que a política de segurança é importante para o sucesso da organização.

FONTE: Nakamura e Geus (2007, p. 197)

7 IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA

A implementação pode ser considerada a parte mais difícil da política de segurança. Sua criação e definição envolvem conhecimentos abrangentes de segurança, ambiente de rede, organização, cultura, pessoas e tecnologias, sendo uma tarefa complexa e trabalhosa. Porém, a dificuldade maior reside na implementação dessa política criada, quando todos os usuários da organização devem ter o conhecimento da referida política, todas as mudanças sugeridas devem ser implementadas e aceitas por todos e todos os controles definidos devem ser implantados com sucesso. Isso faz com que um ponto importante para a aceitação e conformidade com a política definida seja a educação, pois a falta de conscientização dos funcionários acerca da importância e relevância da política é torná-la inoperante ou reduzir sua eficácia. (NAKAMURA; GEUS, 2007, p. 198-199).

> É importante que a empresa disponha de uma política de segurança atualizada e alinhada às necessidades e estratégias do negócio, mas é fundamental que ela seja reconhecida pelos funcionários como o manual de segurança da empresa. Suas diretrizes devem ser conhecidas por todos, e suas normas, procedimentos e instruções específicas devem ser apresentados a cada grupo com perfil de atividade semelhante. Desta forma, cada membro percebe suas responsabilidades dentro de um modelo de segurança único, motivando-o a colaborar. Mas não é suficiente. Lembre-se de que os resultados efetivos de comprometimento ocorrem lentamente e, muitas vezes, requerem ações complementares. (SÊMOLA, 2003, p. 130).

De acordo com Nakamura e Geus (2007, p. 199), com a divulgação efetiva, a política de segurança deverá tornar-se parte da cultura da organização, disseminando as regras estruturais e os controles básicos da segurança da informação no contexto da organização e conscientizando a todos. Alguns exemplos de formas de divulgação que podem ser utilizadas são:

- Comunicação interna (*e-mails*, painéis, páginas na intranet).
- Reuniões de divulgação e conscientização.
- Treinamento específico ou inclusão em programas vigentes.
- Dramatização de exemplos práticos em curtas peças teatrais.
- Incorporação ao programa de recepção a novos funcionários.
- Pôsteres, protetores de tela e *mouse pad* podem ser utilizados para oferecer dicas de segurança, lembrando a todos da importância da segurança de informações.

Sob a ótica da auditoria de sistemas, de acordo com Schmidt, Santos e Arima (2006, p. 43-44), devem ser observados os seguintes aspectos:

- Divulgação formal da política de segurança aos funcionários, terceiros e prestadores de serviços.
- Monitoramento da adoção, cumprimento, atualização e acompanhamento da política de segurança determinada pela alta administração.
- Assinatura de "Termo de Compromisso" relacionado com a confidencialidade das informações, códigos de identificação, senhas de acesso, utilização de ativos, responsabilidades quanto à segurança e ciência das punições para os casos de não aderência às políticas, com envolvimento direto do departamento jurídico na ocasião de sua elaboração.

"Além dos programas de divulgação e conscientização, os executivos devem seguir fielmente a política e valorizá-la, servindo de exemplo para todos os demais". (NAKAMURA; GEUS, 2007, p. 199).

"Os esforços necessários para a implantação da segurança podem levar anos até que se consiga o resultado esperado, o que faz com que um planejamento a longo prazo seja essencial, bem como a aprovação formal de todos os seus passos". (NAKAMURA; GEUS, 2007, p. 199).

Assim, segundo Nakamura e Geus (2007, p. 199), "o ideal é que a segurança tenha seu 'espaço' determinado no orçamento das organizações, com seus devidos planejamentos, equipes e dependências. Além disso, é interessante que ela seja considerada como uma área funcional da organização, como a área financeira ou a área de *marketing*, afinal, a segurança é cada vez mais estratégica para todas as organizações, principalmente em ambientes cooperativos".

> Um ponto importante quanto à política de segurança é que, ao contrário da percepção inicial, seu desenvolvimento ajuda a diminuir, e não a aumentar, os custos operacionais. Isso ocorre porque a especificação dos recursos a serem protegidos, dos controles e das tecnologias necessárias, e de seus respectivos valores, resulta em um melhor controle. Além disso, ela também possibilita o gerenciamento da segurança em nível organizacional, em oposição à dificuldade de gerenciamento de soluções isoladas de fornecedores aleatórios. (NAKAMURA; GEUS, 2007, p. 199-200).

Uma vez que todos os funcionários da organização conheçam a sua política de segurança e passem a aplicá-la, é necessário que as ações de todos passem a ser verificadas quanto à conformidade com a política definida. Isso pode ser feito com auditorias periódicas, que devem ser independentes das pessoas que a estarão implementando.

A política de segurança deve ser aplicada de maneira rigorosa e a não conformidade deve ser punida, de acordo com as ações disciplinares previstas na política.

Além da auditoria, o monitoramento e a revisão da política são importantes para a melhoria contínua dos procedimentos de segurança da organização, assim como são necessários em caso de qualquer mudança que venha a afetar a análise de risco original, tal como um incidente de segurança significativo, surgimento de novas vulnerabilidades, mudanças organizacionais ou na infraestrutura técnica utilizada, que são comuns em ambientes cooperativos.

Com o passar do tempo, é crucial a manutenção da relevância dos pontos da política de segurança: novos pontos podem ser adicionados, quando necessário, como também devem ser removidos os pontos que se tornarem obsoletos.

FONTE: Nakamura e Geus (2007, p. 200)

8 MAIORES OBSTÁCULOS PARA IMPLEMENTAÇÃO DA POLÍTICA

De acordo com Nakamura e Geus (2007, p. 200), "além da dificuldade natural pertinente à implementação da segurança, diversos outros obstáculos podem surgir durante o projeto da política de segurança".

A falta de verbas é o obstáculo mais comum, porém, o fato é que, muitas vezes, isso é apenas uma desculpa, utilizada para que as razões verdadeiras não sejam reveladas. O fato de não conseguir os recursos necessários reflete, fundamentalmente, a falha em convencer os executivos da importância das informações e dos sistemas de informações da organização, que devem, portanto, ser protegidos. Uma maneira prática e comum, porém questionável, de conscientizar os executivos sobre este problema é uma simulação de ataque, que deve, necessariamente, ser realizado somente após uma aprovação prévia por escrito. Além disso, a indisponibilidade de recursos significa prejuízos, pois os negócios podem ser interrompidos como decorrência de um ataque.

Outro obstáculo é a dificuldade dos executivos em compreender os reais benefícios da política de segurança para a organização. Essa política

é um meio de assegurar que os objetivos de gerenciamento sejam seguidos consistentemente dentro da organização, de tal modo que esses executivos devem ter consciência de que, se a política for adotada, seu próprio trabalho ficará consideravelmente mais fácil. Ao fazer com que a implementação da política seja, explicitamente, parte do projeto, existe a possibilidade de descrever os benefícios trazidos com a política de segurança. Por isso, é necessário tratar essa implementação como um assunto específico, que precisa, também, da aprovação dos executivos.

É preciso que os executivos tenham total compreensão de que somente aprovar e publicar os documentos referentes à política desenvolvida não é suficiente. Essa compreensão é importante para evitar que os demais funcionários da organização tenham uma má impressão de descaso por parte dos executivos. A implementação da política desenvolvida requer recursos para o suporte técnico, para os programas de conscientização e treinamento dos usuários, para a substituição e compra de tecnologia e para o estabelecimento de procedimentos adicionais. Por isso, é importante que a implementação faça parte do projeto global de segurança.

FONTE: Nakamura e Geus (2007, p. 201)

> Os executivos podem aprovar uma política de segurança apenas para satisfazer os auditores, e isso acaba comprometendo a própria organização, que pode obter uma política incoerente e sem os detalhes essenciais para o seu sucesso. Esse tipo de comportamento faz com que os executivos devam ser convencidos de que o melhor a fazer é atuar de modo proativo, em oposição ao comportamento reativo. Sendo reativos, em caso de algum incidente de segurança, os executivos serão obrigados a agir em circunstâncias negativas e de extrema urgência e pressão, trazendo, como principal consequência, problemas quanto à confiança de clientes e de parceiros de negócios, e também como a opinião pública. O ideal é mostrar os estudos que provam que é mais barato considerar a perspectiva de 'prevenir, deter e detectar' do que a de 'corrigir e recuperar'. (NAKAMURA; GEUS, 2007, p. 202).

As dependências existentes nos diversos tópicos da política, das normas e dos procedimentos devem ser consideradas para que não sejam feitos esforços em vão. Por exemplo, uma política que torna obrigatório o uso de uma autenticação eficiente para todo acesso remoto deve tratar também dos aspectos que dela dependem, como a arquitetura da solução e dos produtos-padrão a serem utilizados. Sem isso, sua implementação fica comprometida; os usuários irão reclamar que não conseguem trabalhar remotamente (comprometendo sua produtividade) e os executivos, por sua vez, irão reclamar que os usuários não podem trabalhar remotamente, porque não existe a tecnologia que possibilita o acesso remoto seguro (NAKAMURA; GEUS, 2007).

Uma visão abrangente dos problemas relacionados à segurança, juntamente com o conhecimento dos processos de negócios da organização, é fundamental para o desenvolvimento da política. É imprescindível que exista um líder técnico, que seja profundo conhecedor dos aspectos de segurança e tenha uma visão sobre

as tendências e tecnologias nessa área, a fim de possibilitar a implementação das normas e dos procedimentos definidos na política (NAKAMURA; GEUS, 2007).

> É necessário conhecer a complexidade que envolve a rede e os sistemas de informação, para que os recursos adequados sejam alocados no desenvolvimento da política de segurança. O fato de algum desses aspectos serem complexos não significa que deva ser ignorado. Para tanto, é preciso recorrer ao auxílio de ferramentas para a realização dessa tarefa, tais como um *software* de planejamento de contingência. Essa mesma complexidade exige que a organização aloque recursos para sistemas de gerenciamento de redes, sistemas de detecção de intrusões, sistemas de automação e distribuição de *software*, sistemas de checagem de licenças de *software* e outros mecanismos de automação, os quais as pessoas não podem realizar sozinhas. É importante demonstrar para os executivos as novas ferramentas existentes e o porquê de sua popularidade, a fim de comprovar que essa complexidade específica pode ser gerenciada. (NAKAMURA; GEUS, 2007, p. 202-203).

Alguns executivos podem resistir à implementação da política, por acharem que isso trará ameaças ao seu poder e prestígio. Mostrar a esses executivos a importância da centralização e coordenação da política é essencial, para que eles deem o apoio necessário para o sucesso da implementação. Um caso típico da importância da centralização e padronização refere-se ao controle de acesso, quando uma coordenação adequada evita o caos, os aborrecimentos e o desperdício de esforços para todos os envolvidos (NAKAMURA; GEUS, 2007).

> Geralmente, os executivos não gostam de compartilhar e discutir os detalhes técnicos sobre segurança. Porém, é importante que todos estejam engajados nesse processo, porque os executivos precisam entender que a segurança da organização não terá sucesso se não houver o apoio necessário. Além disso, a participação ativa dos executivos no desenvolvimento e na implementação da política é fundamental para o seu sucesso, principalmente porque diversas decisões de negócios incluídas na política não podem ser tomadas pelo pessoal técnico, mas somente pelos executivos. Um exemplo é a política de privacidade de um site de comércio eletrônico, que demonstra que a segurança é multidisciplinar, requerendo a participação de todos dentro da organização. (NAKAMURA; GEUS, 2007, p. 203).

Um processo disciplinar específico para os casos de não cumprimento da política definida é importante para a organização. Por exemplo, se um usuário cometer um erro, a primeira medida é avisá-lo de sua falta. Se o erro se repetir, o chefe do usuário deve receber um comunicado. Se houver um terceiro erro, o usuário será suspenso por duas semanas e se esse erro persistir, o usuário será demitido. Essa abordagem é crucial para evitar situações em que o usuário seja sumariamente demitido, logo no seu primeiro erro, somente para mostrar aos outros funcionários quem detém o poder na organização (NAKAMURA; GEUS, 2007).

9 ESTRUTURA DE UMA POLÍTICA DE SEGURANÇA

Nakamura e Geus (2007, p. 215) "afirmam que a política de segurança deve refletir a própria organização, seguindo sua estrutura, sua estratégia de negócios, sua cultura organizacional e seus objetivos. Assim, a política de uma organização não pode ser aplicada diretamente em outra organização, apesar de existirem

diversos pontos em comum em uma política". Mesmo em uma multinacional, onde normalmente a matriz define a política e a expande para suas filiais, um processo de tropicalização é importante, pois cada país possui alguns aspectos característicos, como é o caso da legislação.

> Esta seção apresenta um exemplo de estrutura para uma política de segurança, que muda de acordo com cada organização. Essa política, como deve ser muito abrangente e flexível o suficiente para que não sofra alterações frequentes, não deve conter detalhes técnicos específicos de mecanismos a serem utilizados ou procedimentos que devem ser adotados por indivíduos particulares, mas, sim, regras gerais e estruturais que se aplicam ao contexto de toda a organização. Além disso, ela deve ser curta o suficiente para que seja lida e conhecida por todos os funcionários da empresa. Assim, os detalhes necessários são inseridos em normas, procedimentos e políticas específicas para cada caso, como também é demonstrado no exemplo. (NAKAMURA; GEUS, 2007, p. 215).

QUADRO 16 – EXEMPLO DE ESTRUTURA DE POLÍTICA DE SEGURANÇA

1	Introdução
1.1	Política de segurança
1.1.1	Informações gerais
1.1.2	Objetivos
1.2	Estrutura de responsabilidade organizacional
1.2.1.1.1	Serviços de informação corporativos
1.2.1.1.2	Serviços de informação de unidades de negócio
1.2.1.1.3	Organizações internacionais
1.2.1.1.4	Encarregados
1.2.2	Padrões de segurança
1.2.2.1.1	Confidencialidade
1.2.2.1.2	Integridade
1.2.2.1.3	Autorização
1.2.2.1.4	Acesso
1.2.2.1.5	Uso apropriado
1.2.2.1.6	Privacidade dos funcionários
2	Descrição do sistema
2.1	Papel do sistema
2.1.1	Tipo de informação manipulada pelo sistema
2.1.2	Tipos de usuário (administração, usuário normal, controlador de impressão etc.)
2.1.3	Número de usuários
2.1.4	Classificação dos dados (dados acessíveis apenas para o departamento de finanças, se necessário)
2.1.5	Quantidade de dados (número de *bytes*)

2.1.6	Configuração do sistema
2.1.6.1	Número de terminais
2.1.6.2	Número de consoles de controle
2.1.6.3	Número e tipos de terminais (inteligente, ignorante, de impressão etc.)
2.1.6.4	Arranjos para carregamento de mídia
2.1.6.5	*Software* (sistema operacional e versão)
2.1.6.6	Interconexões (LAN e WAN)
3	Requisitos de segurança e medidas
3.1	Ameaças à confidencialidade, integridade e disponibilidade dos dados
3.2	Natureza e recursos de possíveis atacantes e atratividade do sistema e dos dados como alvo
3.3	Impactos do comprometimento acidental dos dados
4	Plano de resposta a incidentes de segurança
4.1	Preparação e planejamento da resposta a incidentes
4.2	Notificação e pontos de contato
4.3	Identificação de um incidente
4.4	Resposta a um incidente
4.5	Consequências de um incidente
4.6	Forense computacional e implicações legais
4.7	Contatos de relações públicas
4.8	Passos-chave
4.8.1	Contenção
4.8.2	Erradicação
4.8.3	Recuperação
4.8.4	Acompanhamento
4.8.5	Consequências/Lições aprendidas
4.9	Responsabilidades
5	Contatos e outros recursos
6	Referências

FONTE: Adaptado de Nakamura e Geus (2007, p. 216-217)

LEITURA COMPLEMENTAR

Seu plano de continuidade operacional é pra valer?

Edison Fontes

O desenvolvimento de ações para garantir a continuidade operacional considerando situações de desastre e contingência tem crescido nestes últimos anos em nosso país. Mas, sem tomar uma posição de pessimismo, julgo que ainda é pouco, considerando a quantidade de organizações que fazem o Brasil funcionar. Mesmo assim, muitas daquelas que desenvolvem planos, processos e procedimentos para situações de indisponibilidade dos recursos de informação falham em relação a alguns aspectos ou abordagens para a solução efetiva do problema. Podemos destacar alguns desses aspectos:

1) Somente por causa da legislação

O desenvolvimento de planos de continuidade começou a existir mais fortemente a partir de exigência da legislação nacional ou internacional (para aquelas organizações que possuem ações em Bolsas no exterior). Este fato não é mal, porém é necessário avaliar friamente, de preferência por profissional independente se o que está sendo implementado é um plano efetivo para continuidade operacional ou é apenas um documento para ser verificado em auditorias ou situação similar. O patrocinador desse plano dentro da organização já indica o nível de seriedade com que se deseja implementar a solução. Quanto maior o poder hierárquico desse patrocinador, maior será a concretização efetiva do plano de continuidade operacional.

2) Muita economia financeira

Economia de recursos financeiros é sempre válida, porém não se pode buscar apenas o menor preço em um elemento da solução quando todo o restante da solução tem um padrão de excelência. Faz-se uma instalação elétrica de referência internacional e no final coloca-se tomadas de terceira categoria. Pode ser que na sua organização não aconteça isto, mas acredite que isto acontece em muitas organizações. Planos de continuidade não podem falhar por causa de uma economia do departamento de compras que estava olhando apenas a árvore e não contemplava toda a floresta.

3) Escopo da solução

Na maioria das vezes o executivo não conhece o escopo dos riscos que a solução desenvolvida para situações de contingência abrange. Neste caso o executivo está consciente da necessidade de planos para situações de indisponibilidade, aprovou o orçamento apresentado e. pensa que a sua organização está protegida para todas as situações. Na realidade a organização está protegida para um conjunto de ameaças. É de responsabilidade do profissional de segurança esclarecer

formalmente que cenários e que situações são cobertos na solução implementada. Por exemplo, a organização tem dois locais distintos e distantes de processamento de informações. Esse patamar de proteção contempla a maioria de situações de desastre ou contingência, porém, não será suficiente para uma situação de sabotagem, onde os malfeitores sabem da existência dos dois locais e executarão a sabotagem nos dois locais. A questão a ser decidida é: a ameaça sabotagem deve ser considerada nesta versão do plano?

4) Confiança no parceiro

Evidentemente ter parceiro de renome e reconhecidamente de confiança pelo mercado é um fator que minimiza riscos. Porém, profissionalmente não podemos apenas acreditar que o parceiro tem uma solução para situações de indisponibilidade dos seus recursos. Recursos esses que afetam diretamente o funcionamento da nossa organização. Devemos verificar se possível, através de uma auditoria independente por empresa ou profissional especializado. Essa avaliação deve chegar até o ponto de fazermos testes e simulações em conjunto. Parceria exige confiança dentro de um profissionalismo saudável.

5) Planos de continuidade não são caros ou baratos

Planos de continuidade não são caros ou baratos. Eles devem ser adequados ao porte e tipo de negócio da organização. Evidentemente se uma organização de grande porte, de atuação nacional com um alto nível de exigência para recuperação desenvolver e implementar um plano cujo custo é de milhares de dólares, algo está errado. Este é um plano para milhões de dólares. Mas isto não quer dizer que pequenas empresas ou mesmo nós como pessoa física não podemos ter o nosso plano para enfrentar situações de contingência. Tenho absoluta convicção de que todas as organizações e todas as pessoas que possuem computadores têm recursos para implementar um plano de continuidade operacional adequado às suas necessidades.

6) Plano para situações de contingência faz parte do processo de segurança da informação

Não se deve deixar de considerar que o plano para situações de contingência é um aspecto do processo de segurança. Sendo assim existem outros elementos do processo de segurança da informação que são tão importantes quanto o plano para continuidade operacional. Esses elementos são elos que constroem a corrente da segurança. Se um elo falhar, a corrente rompe e compromete toda a proteção da informação. Controle de acesso à informação e conscientização dos usuários são dois exemplos de elementos críticos para a proteção da informação.

7) Devemos buscar o erro zero

Exagero? Não! Podemos nos espelhar em um exemplo de segurança física, citado no excelente livro Black Box de Gianfranco Beting, lançado neste mês de março em São Paulo, a quem tive o prazer de conhecer: "A Air BP, uma empresa

que distribui e comercializa combustível e lubrificante para o setor aeronáutico tem um único compromisso: nenhum acidente, nenhum dano às pessoas, nenhum dano ao meio ambiente." O enfoque do livro é para a aviação, mas o aprendizado é para todas as áreas. A dependência que as organizações possuem dos recursos de informação já exigem programas sem erros e processos para garantir a continuidade operacional da organização quando de situações de contingência.

8) O teste é para todos

É fundamental a participação da área executiva nas atividades de teste para que todas as pessoas da organização entendam que as regras e os procedimentos foram criados para todos os usuários dos sistemas de informação. A quantidade de testes e a documentação do teste permitindo que o próximo teste seja melhor do que o atual é uma boa dica de que a organização busca a continuidade operacional quando da ocorrência de situação de contingência ou desastre.

Não devemos ficar neuróticos e amedrontados pelas situações de contingência que podem acontecer, porém, profissionalmente devemos analisar todas as ameaças, desenvolver ações que minimizem o risco dessas ameaças e explicitar para o executivo qual o escopo e cenário de contingência para os quais a organização está preparada. Não é uma tarefa fácil além de ser um longo caminho a percorrer. Mas, como em situações desse tipo o mais importante é começar, progredir sempre e ter a visão holística da prática da segurança da informação.
* Consultor, professor e autor de livros de segurança da informação. *E-mail*: edison@pobox.com.

FONTE: FONTES, Edison. CISM, CISA. Disponível em: <http://www.viaseg.com.br/artigo/122-seu_plano_de_continuidade_operacional_e_pra_valer.html>. Acesso em: 24 jul. 2013.

RESUMO DO TÓPICO 3

Caro(a) acadêmico(a)! Neste tópico, você estudou que:

- Todos os usuários de informações e sistemas de informações na organização precisam conhecer seus papeis e responsabilidades para proteger os ativos da empresa.

- Uma política de segurança é um documento que registra os princípios de segurança adotados pela organização e que devem ser observados por todos os colaboradores.

- A política de segurança estabelece linhas-mestres que devem ser seguidas no processo de implementação da segurança da informação, formalizando aspectos para proteção, controle e monitoramento dos ativos de informações.

- A política de segurança é subdividida em três blocos: diretrizes, normas, procedimentos e instruções, sendo destinados, respectivamente, às camadas estratégica, tática e operacional.

- As diretrizes precisam expressar a importância que a empresa dá para a informação. As normas detalham situações, ambientes, processos específicos e fornecendo orientação para o uso adequado das informações. Já os procedimentos e instruções descrevem cada ação e atividade associada a cada situação distinta de uso das informações.

- A política de segurança é o principal elemento para a segurança de qualquer empresa. É o elemento que orienta as ações e as implementações futuras de uma maneira global.

- Quando uma política de segurança é planejada e definida, os executivos demonstram claramente o seu comprometimento e apoio à segurança da informação de toda a organização.

- Os elementos que uma política de segurança adequada deve possuir dizem respeito a tudo aquilo que é essencial para o combate às adversidades.

- Com a divulgação efetiva da política de segurança esta se torna parte da cultura organizacional, disseminando regras estruturais e controles básicos da segurança da informação no contexto da organização.

- Antes de desenvolver a política de segurança, os responsáveis pela sua criação devem ter conhecimento dos diversos aspectos de segurança, além da familiarização com questões culturais, sociais e pessoais que envolvem o bom funcionamento da organização.

AUTOATIVIDADE

1 Quais camadas da estrutura organizacional são contempladas pelos três blocos que compõem a política de segurança, ou seja, diretrizes, normas, procedimentos e instruções?

2 Quais são os quatro elementos essenciais para a definição da política de segurança e para sua implantação, e o que representa cada um destes?

3 Cite três considerações sobre segurança que são importantes para definir uma boa política de segurança.

4 Cite três exemplos de formas de divulgação da política de segurança que podem ser utilizadas pelas organizações.

5 Comente dois obstáculos que podem surgir durante o projeto da política de segurança.

Assista ao vídeo de resolução da questão 4

UNIDADE 3

AUDITORIA DE SISTEMAS

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, será possível:

- entender a origem, os objetivos, os principais fatores motivadores, a estrutura das equipes envolvidas, os controles inerentes ao processo de auditoria de sistemas e as principais técnicas e práticas utilizadas pelas organizações em auditorias de sistemas;

- compreender os mais diferentes tipos de auditorias que podem ser realizadas nas organizações, visando avaliar os processos de desenvolvimento, implantação e utilização da tecnologia da informação;

- conhecer as principais normas e padrões de segurança, nacionais e internacionais, bem como os benefícios advindos da adoção de uma destas pelas organizações.

PLANO DE ESTUDOS

Esta unidade está dividida em três tópicos, sendo que ao final de cada um deles, você encontrará atividades que auxiliarão na apropriação dos conhecimentos.

TÓPICO 1 – FUNDAMENTOS DE AUDITORIA DE SISTEMAS

TÓPICO 2 – TIPOS DE AUDITORIAS

TÓPICO 3 – NORMAS E PADRÕES DE SEGURANÇA

Assista ao vídeo desta unidade.

TÓPICO 1

FUNDAMENTOS DE AUDITORIA DE SISTEMAS

1 INTRODUÇÃO

"Todo sistema está sujeito a falhas, erros e mal uso de recursos em geral. Tanto o computador como a mente humana são instrumentos para grandes realizações, porém não são infalíveis". (SCHMIDT; SANTOS; ARIMA, 2006, p. 11).

Devido à existência desse risco, administradores e proprietários de pequenas e grandes empresas devem, de acordo com Schmidt, Santos e Arima (2006, p. 11), "ter um interesse comum pela manutenção da integridade dos sistemas e das pessoas envolvidas no ambiente de tecnologia de informação".

O sistema de informação é um grande e valioso recurso para a organização. Segundo Schmidt, Santos e Arima (2006, p. 11), "para que ele seja utilizado da melhor forma possível e esteja protegido contra eventuais atos de violação e sinistros, é necessário que os controles sejam considerados desde a fase de concepção".

Ainda de acordo com Schmidt, Santos e Arima (2006, p. 11),

> todos os controles são ferramentas que podem estar integradas ou não a determinado sistema de informação aplicativo, visando à obtenção de segurança contra as ameaças presentes ou potenciais no ambiente de informática. A garantia de funcionamento desses controles, bem como da revisão e avaliação do controle interno, por sua vez, é resultado do bom trabalho de auditoria.

2 CONCEITOS DE AUDITORIA DA TECNOLOGIA DE SISTEMAS

A auditoria em ambiente de tecnologia de informação não muda a formação exigida para a profissão de auditor, apenas percebe que as informações até então disponíveis em forma de papel são agora guardadas em forma eletrônica e que o enfoque de auditoria, segundo Imoniana (2011, p. 16) "teria que mudar para se assegurar de que essas informações em forma eletrônica sejam confiáveis antes de emitir sua opinião".

De acordo com Imoniana (2011, p. 17), "a filosofia da auditoria de tecnologia de informação está calçada em confiança e em controles internos. Estes visam confirmar se os controles internos foram implementados e se existem. Caso existam, então é verificado se eles são efetivos".

As atividades de auditoria de tecnologia de informações, além de tentar utilizar os recursos de informática para auditar o próprio computador, também visam automatizar todos os processos de auditoria. Imoniana (2011, p. 17) comenta que como em qualquer outra atividade, as empresas de auditoria também buscam um diferencial competitivo. Entre outros objetivos, são considerados:

a) Melhorar a eficiência e reduzir os custos.
b) Melhorar a qualidade do trabalho de auditoria, reduzindo, assim, os níveis de risco de auditoria.
c) Atender às expectativas dos clientes, que esperam de seus auditores o mesmo grau de automatização que utilizam em seu próprio negócio.
d) Preparar-se para a globalização dos negócios, que vem exigindo uma globalização dos auditores.
e) Manter-se entre as maiores e mais reconhecidas pelo mercado.

Schmidt, Santos e Arima (2006, p. 19) afirmam que geralmente, os objetivos da auditoria têm em vista:

a) Assegurar a adequação do sistema de controles que está implantado e que está sendo utilizado.
b) Determinar se os recursos estão sendo utilizados em função da análise de custo e benefício.
c) Checar se os ativos estão salvaguardados apropriadamente.
d) Revisar a integridade, confiabilidade e eficiência do sistema de informação e dos relatórios financeiros nele produzidos.

De acordo com Imoniana (2011, p. 17), os benefícios da automação compreendem:

- Treinamento de pessoal e superação de resistências à tecnologia.
- Decisões de quais tarefas devem ser automatizadas primeiro.
- Avaliação, escolha e implantação de *softwares* e *hardwares*.
- Gerenciamento de arquivos eletrônicos: dispositivos de segurança e *backup*.
- Disponibilização de equipamentos para toda a equipe de auditores, podendo trabalhar em redes.
- Instalação e manutenção de uma malha de comunicações.
- Maior transferência de conhecimento entre os membros da equipe e entre trabalhos de equipes diferentes.

- Independência das limitações impostas pelos arquivos de auditoria em papel.
- Economia de tempo das atualizações.
- Melhor qualidade na apresentação.
- Liberação de funcionários mais experientes para que se dediquem a áreas mais técnicas e de maior risco.
- Agregação de valor ao trabalho de auditoria.
- Formação de equipes virtuais (*groupware*), maximizando a especialização.
- Fluxo de informações mais rápido.
- Maior satisfação profissional.
- Maior respeito pelo auditado.
- Maior produtividade.
- Realização das tarefas sem a automatização pelos profissionais menos experientes. Antes, somente, poderiam ser executadas por profissionais mais experientes.

3 ABORDAGEM DE AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Para auditar as informações em ambiente de TI, o auditor poderá desenhar as abordagens que lhe convêm. Segundo Imoniana (2011, p. 18), "as abordagens mais comuns são: abordagens ao redor do computador, através do computador e com o computador".

A auditoria tradicional sempre foi conhecida por sua responsabilidade nos testes de confiabilidade dos registros de acordo com os documentos-fonte (os documentos que geram todas as transações econômicas, financeiras e contábeis) disponíveis através de quaisquer dados intermediários que possam existir e para os quais são produzidos relatórios para a tomada de decisões gerenciais. Porém, conforme Imoniana (2011, p. 18), "devido à evolução das tecnologias de informação, que interfere nas tecnologias gerenciais, geração a geração, é necessário guardar as informações para que sejam acessíveis para auditoria quando forem requisitadas". Sabe-se que, devido à complexidade dos ambientes e expansão dos negócios que atingiram implementações em ambiente de intranet e internet, há grandes problemas quanto à vulnerabilidade de computadores e alguns casos comuns de fraudes.

Imoniana (2011, p. 18) comenta que, dependendo da sofisticação do sistema computadorizado, em que se supõe que o auditor seja operativo, e considerando as características do auditor de tecnologia de informações, este pode usar qualquer das três abordagens nomeadas a seguir:

1. Abordagem ao redor do computador.
2. Abordagem através do computador.
3. Abordagem com o computador.

3.1 ABORDAGEM AO REDOR DO COMPUTADOR

Auditoria ao redor do computador, no passado, era uma abordagem muito solicitada pelos auditores, devido ao não envolvimento de muita tecnologia de informação. De acordo com Imoniana (2011, p. 19), "a abordagem requer que o auditor examine os níveis de anuência associados à aplicação dos controles organizacionais, no que concerne à tecnologia de informação".

Isso significa a auditoria de documentos-fonte com as funções de entrada subjacentes e dominando as funções de saída, que se encontram em formatos de linguagem legível por leigos em informática. Segundo Imoniana (2011, p. 19),

> O sistema de processamento eletrônico de dados nesta era foi somente usado para tarefas menores, tais como obtenção de níveis de estoque e sugestões para realimentação quando forem reais. As operações simples, tais como o isolamento de estoques com pouca movimentação e estoques obsoletos, são executadas pelos computadores às funções de impressão dos relatórios.

Há, geralmente, um questionamento quanto à operação deste método, no qual, se indaga se é de fato uma boa prática de auditoria. Todavia, a dificuldade para decidir deu-se devido à capacidade de tais sistemas serem programados para executar operações contábeis simples e os auditores conduzirem como tarefas, avaliando simples entradas e saídas dos sistemas. Para Imoniana (2011, p. 19), deve-se notar que, "apesar de essa abordagem não ser tão apropriada para ambientes complexos, ela ainda é bastante conveniente para sistemas menores, onde a maior parte das atividades de rotina é executada manualmente".

De acordo com Imoniana (2011, p. 19), as vantagens associadas ao uso desta abordagem são:

a) Não exige conhecimento extenso de tecnologia de informação para que o auditor possa operar convenientemente este método, e isto faz com que as técnicas e ferramentas de auditoria sejam válidas.

b) Também sua aplicação envolve custos baixos e diretos.

Ainda de acordo com Imoniana (2011, p. 20), as desvantagens no uso desta abordagem são:

a) Restrição operacional quanto ao conhecimento de como os dados são atualizados faz com que a auditoria seja incompleta e inconsistente, uma vez que o processo operacional é dinâmico, atendendo às necessidades sociais.
b) A eficiência operacional de auditoria pode ser avaliada com maior dificuldade, visto que não há parâmetros claros e padronizados.
c) Uma vez não sendo necessária que o auditor possua maior capacidade profissional adequada, no que se refere à tecnologia de informação, para capacitá-lo a executar uma revisão mais lógica, o sistema pode ser enquadrado em limites de grande risco, quando houver uma evolução e os documentos-fonte saírem de seu controle.
d) As avaliações de tecnologia de informações, seja ambiente de uso pequeno, significativo ou complexo, não importa, se executar algum procedimento de auditoria que exclua as Unidades Centrais de Processamento (CPU) e suas funções aritmética a lógica, não podemos afirmar que tal abordagem de auditoria tenha sido representativa e global de toda tecnologia de informação daquela organização. Assim, as decisões tomadas baseadas em relatórios de tais auditorias podem ser distorcidas.

3.2 ABORDAGEM ATRAVÉS DO COMPUTADOR

O uso desta abordagem envolve mais do que mera confrontação de documentos-fonte com os resultados esperados, uma vez que os sistemas têm evoluído muito. No entanto, segundo Imoniana (2011, p. 20), "este método alerta quanto ao manuseio de dados, aprovação e registro de transações comerciais, sem deixar evidências documentais razoáveis através dos controles de programas construídos junto aos sistemas". Por esta razão o auditor precisa acompanhar o processamento através de dentro do computador.

A abordagem melhora o método de auditoria ao redor do computador. Assim, auditando com este método, uma pessoa poderia requisitar, de muitas maneiras, como é praticada na abordagem ao redor do computador, a verificação dos documentos-fonte com dados intermediários. Porém, de acordo com Imoniana (2011, p. 20), estabelece ao auditor uma maior ênfase em todas as técnicas que utilizam o computador como uma ferramenta para testar a si próprio e, também, testar uma entrada de dados.

As pessoas a favor do uso de abordagem através do computador apoiam o uso de *test data*. Para Imoniana (2011, p. 20) "é o processamento de um dispositivo capaz de simular todas as transações possíveis".

Imoniana (2011, p. 21) indica as seguintes vantagens quanto ao uso desta abordagem:

a) Capacita melhor o auditor a respeito de habilidade profissional no que tange a conhecimento de processamento eletrônico de dados.
b) Capacita o auditor a verificar com maior frequência as áreas que necessitam de revisão constante.

As desvantagens desta abordagem, segundo Imoniana (2011, p. 20) são:

a) Se a operação for efetuada incorretamente, pode levar a perdas incalculáveis.
b) O uso da abordagem pode ser caro, principalmente no que diz respeito ao treinamento de auditores, aquisição e manutenção dos pacotes de *software*.
c) Partindo do pressuposto de que os pacotes são completos, podem estar errados. As técnicas manuais podem ser necessárias como complementos para que a abordagem funcione efetivamente.
d) Há risco de que os pacotes possam estar contaminados pelo uso frequente na auditoria organizacional.

3.3 ABORDAGEM COM O COMPUTADOR

A primeira abordagem, ao redor do computador, de acordo com Imoniana (2011, p. 21), "não é eficiente devido ao fato de que negligencia algumas das qualidades dos controles internos dos sistemas e propicia falta de disponibilidade de testes substantivos convincentes que visam ajudar na conclusão sobre os sistemas".

Ainda conforme Imoniana (2011, p. 21), "a segunda abordagem, através do computador, preferida como superior à primeira, pode também produzir registros incompletos. Ao invés de efetuar uma verificação de equilíbrio com as ferramentas, ela tende a negligenciar os procedimentos manuais, deixando incompleta a maioria das tarefas normalmente efetuadas manualmente".

Devido a estas razões, Imoniana (2011, p. 21) afirma que "as empresas de auditoria e pesquisadores da área contábil propuseram um meio de auditar as tecnologias de informação com a maior perfeição possível, utilizando a abordagem com o computador completamente assistida".

Fazendo uma síntese do processo, alguns objetivos têm sido alcançados. São eles:

a) A utilização das capacidades lógicas e aritméticas do computador para verificar se os cálculos das transações econômicas e financeiras ou aqueles que dizem respeito às responsabilidades, como, por exemplo, o cálculo das depreciações, taxas e impostos, multiplicações e contabilizações (*footings*), são feitos corretamente.
b) A utilização das capacidades de cálculos estatísticos e de geração de amostras que facilitem confirmações de saldos necessárias para aferir a integridade de dados de contas a receber, estoques imobilizados, advogados, entre outros.
c) A utilização de capacidades de edição e classificação do sistema computadorizado, a fim de ordenar e selecionar os registros de contabilidade. Por exemplo, através de varredura de base de dados de sistema de estoque, um auditor pode ser capaz

de apontar com precisão os itens de movimento mais vagarosos, obsoletos, e isolá-los dos itens de movimentos rápidos, para facilitar análises mais complexas e substantivas.

d) A utilização das capacidades matemáticas do computador para analisar e fornecer listas de amostras de auditoria. Pode, também, incluir a confirmação dos resultados de auditoria executada manualmente, como dos cálculos globais.

Uma grande facilidade do uso desta abordagem, de acordo com Imoniana (2011, p. 22) é a disponibilidade e uso vantajoso de:

a) Capacidades de auditoria de aplicar Técnicas de Auditoria Assistida por Computadores (TAAC), em outro momento chamadas CAAT (*Computer Assisted Audit Techniques*).
b) Possibilidades de desenvolver programas específicos para serem usados pelo auditor quando da necessidade de evidenciar uma opinião sobre o processo contábil.
c) Ganhar tempo sobre os passos aplicados com o uso de pacote generalizado de auditoria de tecnologia de informação.

4 ORGANIZAÇÃO DE TRABALHO DA AUDITORIA DE TI

O processo de organização dos trabalhos de auditoria de tecnologia de informações segue a norma de execução de trabalhos, o principal componente das normas de auditoria geralmente aceitas. Segundo Imoniana (2011, p. 22), essa norma contempla:

- Planejamento de auditoria.
- Avaliação de riscos de auditoria.
- Supervisão e controle de qualidade.
- Estudo e avaliação do sistema contábil e de controles internos e aplicação dos procedimentos de auditoria.
- Documentação da auditoria.
- Avaliação da continuidade normal dos negócios da entidade.
- Aplicação de amostragens estatísticas.

4.1 PLANEJAMENTO

A atividade de planejamento em auditoria de sistemas de informações é imprescindível para melhor orientar o desenvolvimento dos trabalhos. De acordo com Imoniana (2011, p. 23),

> como o trabalho de auditoria representa processo contínuo de avaliação de risco ao qual se adicionam as experiências individuais dos profissionais e a evolução da prática e metodologias, aliadas aos resultados dos trabalhos e processos de negócios, anteriormente objetos de avaliação dos auditores, o planejamento é caracterizado para evitar quaisquer surpresas que possam acontecer tanto nas atividades empresariais, objetivo de auditoria, como também em relação à responsabilidade dos auditores.

Ainda de acordo com Imoniana (2011, p. 23),

> desde os primeiros trabalhos deve ser desenhada uma matriz de risco que seja permanentemente atualizada a partir dos resultados obtidos nos testes e nas avaliações dos auditores, assim como do impacto das mudanças ocorridas no negócio resultante de alterações estatutárias, legislações, mudanças nas leis ambientais, social e econômica ou qualquer outro fator que tenha reflexo nas demonstrações financeiras, continuidade operacional, qualidade dos controles e, sobretudo, nos processos operacionais.

4.2 ESCOLHER A EQUIPE

Um planejamento detalhado e atualizado com base nas principais mudanças de negócio permite indicar o perfil básico da equipe de auditoria TI, o qual, segundo Imoniana (2011, p. 25) contempla o seguinte:

a) Perfil e histórico profissional.
b) Experiência acumulada por ramos de atividade.
c) Conhecimentos específicos.
d) Apoio do grupo de especialização.
e) Formação acadêmica.
f) Línguas estrangeiras.
g) Disponibilidade para viagens etc.

4.3 PROGRAMAR A EQUIPE

O encarregado de auditoria deve programar a equipe para executar os trabalhos. Para Imoniana (2011, p. 25), a programação de uma equipe de auditores com o perfil adequado para a realização do trabalho previsto não é suficiente para garantir que todos os riscos de auditoria sejam minimizados pelos testes de auditoria, no entanto, devem-se observar as habilidades que permitem:

a) Gerar programas de trabalho que extraiam dados corretos para testes.
b) Selecionar procedimentos mais apropriados.
c) Incluir novos procedimentos.
d) Classificar trabalhos por visita.
e) Orçar tempo e registrar o real.
f) Evidenciar corretamente os trabalhos realizados; utilizando-se *softwares* de amostragens estatísticas, entre outros, para otimizar os trabalhos.
g) Gerar relatórios em consonância com os trabalhos efetuados.

4.4 EXECUÇÂO DE TRABALHOS E SUPERVISÃO

As tarefas deverão ser realizadas por auditores que tenham formação, experiência e treinamento adequados no ramo de especialização. Para Imoniana (2011, p. 25),

> dependendo da complexidade do ambiente operacional, aparente risco envolvido, os trabalhos serão desenvolvidos conforme vivência profissional, ou seja, tarefas mais simples e de menor risco serão desempenhadas por membros menos experientes, e tarefas mais complexas ou de maior risco serão de responsabilidade dos membros mais experientes e de melhor formação da equipe.

A questão de supervisão é inerente ao processo de auditoria para garantir a qualidade e certificar que as tarefas foram adequadamente feitas. Isto ainda permite cobrir os riscos prováveis identificados.

4.5 REVISÂO DOS PAPÉIS DE TRABALHOS

Como tarefa para atingir a qualidade exigida pelas práticas de auditoria, os papéis de trabalhos são revisados pelos superiores, que têm a incumbência de assinar junto com seus subordinados o cumprimento de cada passo de auditoria concluído. Segundo Imoniana (2011, p. 26), "eventualmente, em decorrência dos trabalhos de auditoria, falhas ou recomendações para melhorias são identificadas e limitam a conclusão do auditor, assim como determinados procedimentos que não tenham sido cumpridos por restrições do próprio cliente".

No entanto, Imoniana (2011, p. 26) afirma que, "o revisor, não identificando outros passos de auditoria independentes, poderá solicitar uma nova visita para completar os trabalhos". Contudo, para as pendências de revisão, deve ser analisado o reflexo do aumento ou alteração do escopo, novos trabalhos, nova abordagem, impacto no parecer final, na carta de representação da gerência.

4.6 ATUALIZAÇÃO DO CONHECIMENTO PERMANENTE

O conhecimento em determinado período de auditoria, dito como aquele que muda com pouca frequência, sempre é fundamental e serve como ponto de partida para o período subsequente. Para Imoniana (2011, p. 26), "a manutenção em forma eletrônica, a documentação da descrição e a avaliação do ambiente de controle interno, controles gerais e dos sistemas aplicativos e processos de negócios contribuirão para a redução das horas de auditoria do período seguinte".

Para Imoniana (2011, p. 27), entre as informações relevantes destacam-se:

a) Descrição do processo de negócios.
b) Levantamento e avaliação do ambiente de controle.
c) Documentação e conclusão sobre a avaliação dos controles dos processos relevantes.
d) Matriz de risco que pontue riscos aparentes para todos os principais componentes da demonstração financeira.
e) Exceções dos testes.
f) Falhas ou fraquezas nos testes de controles internos.
g) Programas de trabalho.

4.7 AVALIAÇÂO DA EQUIPE

A fim de garantir a evolução e o aprimoramento técnico dos profissionais da equipe de auditoria de TI, Imoniana (2011, p. 27) afirma:

> Deve-se avaliar o desempenho, elogiando os pontos fortes do auditor, auxiliar no reconhecimento das fraquezas e na elaboração de um plano para superá-las para que se desenvolva um profissional qualificado e consciente. Como é de praxe, para cada trabalho no qual um profissional é programado, o sistema que controla a programação emitir eletronicamente uma avaliação de desempenho já preenchida pelo superior, isto é fundamental para nortear a promoção ou não do profissional.

5 DOCUMENTAÇÃO DOS PAPÉIS DE TRABALHO

Os papéis de trabalhos constituem um conjunto de formulários preenchidos logicamente no processo de auditoria de sistemas, com seus anexos, que evidenciem os fatos relatados. "Se esses anexos forem provas documentais, podem ser escaneados para serem documentados eletronicamente. Contêm informações coligidas durante o teste, os procedimentos executados e as opiniões formadas sobre o objeto de auditoria". (IMONIANA, 2011, p. 27).

Os papéis de trabalhos, independentemente de seu enfoque ser sistêmico ou manual, devem ser autossuficientes e não devem necessitar, subsequentemente, de explicações verbais e adicionais do preparador a fim de detalhar a metodologia adotada. Imoniana (2011, p. 27) afirma que, "como o objetivo desta seção se restringe a aspectos de documentação eletrônica de papéis, não estão sendo abordados os critérios minuciosos de elaboração de papéis".

6 DESENVOLVIMENTO DA EQUIPE DE AUDITORIA

"A crescente complexidade dos ambientes de tecnologia de informações tem criado uma preocupação por parte dos usuários dos serviços de auditoria, gerando uma expectativa quanto ao desenvolvimento da capacidade de auditoria para atenuar os riscos, tais como, fraudes intencionais ou não intencionais". (IMONIANA, 2011, p. 33).

No passado recente, os profissionais de auditoria e de tecnologia de informações desenvolveram-se em suas atividades independentes um do outro. No entanto, segundo Imoniana (2011, p. 33), "com as necessidades de sinergias operacionais e a demanda perpétua para interação interdisciplinar, os próprios auditores menos qualificados em questões de tecnologia de informações solicitam apoio dos especialistas em Ciência da Computação para melhor auditar este ambiente. Esses trabalhos em grupo iniciam-se com a avaliação ao redor do computador".

Para que o auditor venha a atuar apropriadamente como auditor de tecnologia de informações, seu *know-how* relativo à tecnologia avançada precisa ser aprimorado. Conforme Imoniana (2011, p. 33), abaixo seguem as estratégias normalmente implementadas para compor a equipe de auditoria de TI:

- Treinar um número de auditores internos ou independentes em conceitos e práticas de tecnologia de informações e métodos para a aplicação das técnicas e ferramentas de auditoria em ambiente computadorizado.
- Treinar alguns analistas de sistemas em prática e princípios de auditoria geral e no uso de técnicas e ferramentas de auditoria.
- Contratar e treinar auditores, fornecendo-lhes tanto conhecimento de auditoria como de tecnologia de informações para compor a equipe desde o início.
- Contratar auditores com larga experiência com objetivo de torná-los auditores de tecnologia de informações.

Geralmente, dificuldades têm sido encontradas pelos auditores com relação às várias estratégias. Para Imoniana (2011, p. 34), "os auditores são céticos e andam com relutância quanto à proposta de se adequarem à tecnologia de informações para

auditar os sistemas computadorizados". Por outro lado, os analistas de sistemas veem a alternativa de estudar a auditoria para atuar como auditor de tecnologia de informações como um redirecionamento de suas carreiras. Entretanto, com ausência de relutância, os auditores sentem-se incumbidos de se atualizar para atender à nova ordem da atuação profissional, ou seja, adquirir um *know-how* de TI.

"Numa outra visão sobre a opção de treinar analistas de sistemas, o profissional não está totalmente maduro por um curto prazo de treinamento para adquirir um senso crítico e de julgamento profissional do auditor, podendo comprometer os propósitos". (IMOANIANA, 2011, p. 34).

7 CONTROLES INTERNOS E AVALIAÇÃO

Segundo o Instituto Americano dos Contadores Públicos Certificados, através do Relatório Especial da Comissão de Procedimentos de Auditoria, controle interno é o "plano de organização e todos os métodos e medidas coordenados, aplicados em uma empresa, a fim de proteger seus bens, conferir a exatidão e a fidelidade de seus dados contábeis, promover a eficiência e estimular a obediência às diretrizes administrativas estabelecidas pela gestão". (SCHMIDT; SANTOS; ARIMA, 2006, p. 12).

Essa definição, de acordo com Schmidt, Santos e Arima (2006, p. 12), identifica a principal estrutura do ciclo gerencial em termos de planejamento, execução e controle, relacionando uma diversidade de meios à disposição da alta administração para a devida aplicação das funções gerenciais dentro da organização.

Ao analisar a extensão dessa definição, Schmidt, Santos e Arima (2006, p. 12) observa a existência dos seguintes itens, ao qual o controle deve atender:

- Proteção dos bens.
- Conferência da exatidão e da fidelidade dos dados contábeis.
- Promoção da eficiência operacional.
- Estímulo à obediência das diretrizes administrativas estabelecidas.

Esses itens, conforme Schmidt, Santos e Arima (2006, p. 12) "possibilitam a determinação de diversos parâmetros de controle interno, permitindo o estabelecimento de objetivos de desenvolvimento do trabalho da auditoria de sistemas".

7.1 FUNDAMENTOS DE CONTROLES INTERNOS EM SI

O conceito de Controle Interno em um sistema de informação, conforme declaração do Instituto Americano de Contadores Públicos, significa "planos organizacionais e coordenação de um conjunto de métodos e medidas adotado numa empresa, a fim de salvaguardar o ativo, verificar a exatidão e veracidade de registros contábeis, promover a efetividade de sistema de informação contábil e eficiência operacional, assim como fomentar uma grande adesão às políticas da organização".

FONTE: Adaptado de: <http://everson.com.br/files/Auditoria%20-%20impress%C3%A3o.pdf>. Acesso em: 14 ago. 2013.

Segundo Imoniana (2011, p. 40), "o uso do computador de forma alguma altera os conceitos básicos de um sistema de controle interno. O que muda são as abordagens diferentes, usadas em um ambiente de tecnologia de informação, distintas das do ambiente manual".

Com o aumento no uso de tecnologia de informações nos negócios, o auditor incorpora a nova tarefa, inclui revisão de controles em sua cobertura de riscos empresariais, assim como enfatiza o evangelho de anuência às características essenciais de controle. Para Imoniana (2011, p. 40), "a auditoria de sistema de controle interno de uma organização inclui verificações dos processos e confirmação quanto à sua efetividade, e é por isso que é regido pela lei da variedade de requisitos". Agora, o problema repousa na semelhança de variedade de sistemas contábeis existentes e seus processos de apoio à decisão gerencial.

Entretanto, esta última característica deveria ser observada se a organização, devido a seu sistema dinâmico operacional claramente definido, tem que manter fidelidade e/ou integridade de informação, eficiente e eficaz. De acordo com Imoniana (2011, p. 40), "a eficácia de um sistema tem sido visualizada quanto ao que concerne à consecução da missão de tecnologia de informação".

"Se o objetivo do sistema for reduzir o headcount ou agilizar o processo de tomada de decisão, este tem que ser atingido, ou o sistema não virá ao encontro da sua expectativa, e pode ser julgado a partir da função de fornecer informação necessária ao processo de tomada de decisão da gerência". (IMONIANA, 2011, p. 41).

Para Imoniana (2011, p. 41), os principais objetivos de um sistema geral de controle interno são:

- Salvaguardar o ativo de uma organização.
- Manter a integridade.
- Correção e confiabilidade dos registros contábeis.
- Promover a eficiência operacional.
- Encorajar o cumprimento dos procedimentos e políticas da gerência.

"Esses objetivos não apresentam diferenças nos procedimentos de controles internos em ambientes de tecnologia de informações". (IMONIANA, 2011, p. 41).

Ao falar sobre princípios de controles internos geralmente aceitos em ambiente de tecnologia de informação, que constituem a parte integral dos objetivos e princípios de controles internos em âmbito global, segundo Imoniana (2011, p. 41), alguns destes princípios estão em operação, dentro dos ambientes computadorizados, e são aceitos em tais ambientes. Dentre eles estão os seguintes:

- Supervisão
  - A gerência por objetivos, procedimentos e tomada de decisões deve manter um controle que a capacite a uma supervisão efetiva dentro do ambiente de tecnologia.
- Registro e comunicação
  - A gerência da empresa deve estabelecer critérios para criação, processamento e disseminação de informação de dados através de autorização e registro de responsabilidade.
- Segregação das funções
  - As responsabilidades e ocupações incompatíveis devem estar segregadas de maneira a minimizar as possibilidades de perpetuação de fraudes e até de suprimir erro e irregularidade na operação normal.
- Classificação de informação
  - A gerência deve estabelecer um plano para classificação de informação que melhor sirva às necessidades da organização, em conformidade com os princípios da contabilidade e também padrões de auditoria geralmente aceitos.

- Tempestividade
  • A gerência deve delinear procedimentos, monitorar os registros corretos das transações econômicas, financeiras e contábeis das empresas, processando-as e comunicando os resultados às pessoas necessárias em tempo hábil.
- Auditoriabilidade
  • Os procedimentos operacionais devem permitir a programação e verificação periódica no que concerne à precisão do processo de processamento de dados e de geração do relatório, de acordo com as políticas.
- Controle independente
  • Os sistemas em funcionamento devem ter procedimentos adequados para identificação e correções de erros no fluxo de processamento, inclusive nos processos executados concomitantemente.
- Monitoramento
  • A gerência deve possuir acesso *master* ao sistema e controle de uso que lhe permita fazer o acompanhamento *pari passu* das transações.
- Implantação
  • A gerência deve planejar a aquisição, o desenvolvimento, a manutenção e a documentação de sistema, de forma a coincidir com as metas empresariais.
- Contingência
  • A gerência deve implementar um plano adequado e procedimentos de implantação para prevenir-se contra as falhas de controles que podem surgir durante especificações de sistema, desenho, programação, testes e documentação de sistemas e nas fases pós-implantações.
- Custo efetivo
  • Investimentos em tecnologia da informação devem ser propriamente planejados, a fim de coincidirem com o custo efetivo.
  • A natureza e extensão de controles necessários em ambiente de tecnologia de informação variam, paulatinamente, de acordo com a complexidade da tecnologia de informação em operação. Para alguém que diligentemente acompanhe o sistema de controle em um ambiente particular, é imperativo que determine e padronize os tipos de equipamentos em operação, a natureza dos dados que são processados e os procedimentos metodológicos existentes. Num ambiente de sistema computadorizado básico, que processe seus dados mais manualmente do que computacionalmente, pode haver uma necessidade de procedimentos tais como: identificação, autorização, autenticação e classificação de dados que sejam realizados manualmente. Evidentemente, o sistema necessitará mais de controles convencionais do que de controles modernos e computadorizados, que são bastante direcionados para ambientes de tecnologia de informação mais complexos.

• Para isso, vários tipos de controles são estabelecidos pela gerência de uma organização para manter uma administração própria de um sistema computadorizado. Eles envolvem os controles organizacionais, controles de segurança e privacidade, controles de preparação, controles de entrada e controles de processamento. Outros são controles de recuperação e armazenamento de dados e controles de saída.

7.2 AVALIAÇÃO DOS CONTROLES INTERNOS

A avaliação dos procedimentos de controles internos em ambientes de sistemas de informações de uma organização é um trabalho executado pelo auditor que tenha habilidade em tecnologia de informações.

No contexto normal de auditoria financeira, ele tem o propósito de certificar a veracidade das demonstrações financeiras para fins de pareceres, quando este examina o nível de aderência aos controles internos em tecnologia de informação na consecução das transações econômicas e financeiras, contábeis, ambiental e social. Envolve os testes de observância e testes substantivos. Os testes de observância fornecem a segurança adequada de que os controles operacionais dos sistemas de informações estão sendo estritamente aderidos. Podem surgir questões a esse respeito como as seguintes:

- Os procedimentos necessários concebidos nos sistemas foram executados?
- Para que foram executados?
- O auditor, quando do início da avaliação dos sistemas, leva em consideração suas conclusões sobre os riscos de controles, a fim de que venha a ter visão preliminar com respeito à efetividade dos controles e de que são confiáveis e possuem um grau razoável de segurança?

FONTE: Imoniana (2011, p. 51)

Supondo que um sistema típico seja colocado em teste de observância, o auditor, então, faz julgamento a partir da evidência que está à sua disposição, a fim de verificar se há necessidade de executar um teste analítico substantivo. Conforme Imoniana (2011, p. 51), "se ocorrer a última probabilidade, o auditor, então, executa os testes preliminares e aprofunda-os em tais áreas".

Para Imoniana (2011, p. 51), "quanto mais fortes os reflexos de controle interno dentro de uma organização, menor será a intensidade dos trabalhos de avaliação dos controles internos e também a relação com a integridade de dados e vice-versa".

Crê-se que os sistemas computadorizados, ao inverso dos sistemas manuais, têm maior consistência, mas estes não excetuam a execução do teste de anuência. Segundo Imoniana (2011, p. 51), "alguém pode sempre pegar alguns dados e traçá-los corretamente a partir do *input*, direcionando-os através do processamento até o *output*, para ver se houve adequado procedimento de processamento e em conformidade com as políticas de gerenciamento".

Para Imoniana (2011, p. 51), "é sabido que alguns destes sistemas são mais vulneráveis do que outros". Por exemplo: consideram-se as fases de manuseio de dados físicos como mais susceptíveis a fraudes por computador do que outros controles, e sugere-se atenção especial no processo de sua avaliação. A discriminação dos subsistemas também não é novidade. Isto tende a atribuir maior importância ao relacionamento entre custos e benefícios de um ponto de controle ao qual se deve prestar mais atenção.

Em qualquer sistema de informação complexo ou moderado, segundo Imoniana (2011, p. 51), "sua avaliação pelos auditores internos se processa através do uso de ferramentas adequadas de auditoria, métodos e técnicas".

Imoniana (2011, p. 52) aconselha que, "para maior eficiência dos trabalhos, sejam concentradas as tarefas de avaliação das atividades de monitoramento geralmente executadas pelos gerentes em níveis hierárquicos estratégicos e táticos e nos procedimentos de controles relacionados com as transações econômicas e financeiras em níveis operacionais".

Imoniana (2011) recomenda testar os controles internos no ínterim, para auxiliar o direcionamento dos trabalhos de testes substantivos e analíticos nos finais. Para os trabalhos de auditoria interna devem-se testar os controles internos, conforme o planejamento dos trabalhos à medida que surjam as necessidades gerenciais.

8 FERRAMENTAS DE AUDITORIA DE TI

O principal objetivo do uso de "Técnicas de Auditoria Assistida por Computador" (TAAC) é, segundo Imoniana (2011, p. 54), "auxiliar o auditor para auditar 100% a população da área ou transação revisada, considerando o limite de tempo que possui, aproveitando os recursos de *softwares* e as técnicas de auditoria em ambiente de computação". Essas técnicas são importantes, pois auxiliam na avaliação deste ambiente, que geralmente processa os volumes de transações muito grandes. Além disso, as trilhas de auditorias nem sempre são visíveis, ou por falta de *hardcopy*, ou em casos de autorizações através de voz, imagens e impressão digital. A simples confirmação de créditos pode não gerar nenhuma trilha de auditoria.

As técnicas de auditoria assistida por computador podem ser aplicadas nas seguintes tarefas:

a) Testes de controles gerais:
   • Testes de configuração de um sistema operacional ou utilizando um *software* de comparação de versões para confirmar se as versões aprovadas são aquelas implementadas e em uso em ambiente de produção.
b) Testes de detalhes de transações
   • Calcular os saldos novamente ou gerar juros sobre uma conta cliente, levando-se em conta todas as características ou fatos que geraram seu lançamento.
c) Analítico e substantivo
   • Identificar inconsistências ou flutuações anormais nas contas e grupos de contas contábeis.
d) Amostragem
   • Gerar amostras para alimentação dos programas de auditoria.

FONTE: Imoniana (2011, p. 54)

"As ferramentas normalmente auxiliam na extração, sorteio, seleção de dados e transações, atentando para as discrepâncias e desvios". (IMONIANA, 2011, p. 55).

8.1 *SOFTWARE* GENERALISTA DE AUDITORIA DE TI

De acordo com Imoniana (2011, p. 55),

> envolve o uso de *software* aplicativo (um conjunto de programas) em ambiente *batch*, que pode processar, além de simulação paralela, uma variedade de funções de auditoria nos formatos que o auditor desejar. As funções são tais como extração de dados de amostra, testes globais, geração de dados estatísticos para análise, sumarização, composição de um outro arquivo a partir de um arquivo mestre de dados, apontamento de duplicidade de registros ou sequência incorreta, entre outras.

Os *softwares* generalistas são:

a) ACL (*Audit Command Language*): é um *software* para extração e análise de dados, desenvolvido no Canadá.
b) IDEA (*Interactive Data Extraction & Analysis*): *software* para extração e análise de dados, também desenvolvido no Canadá.
c) *Audimation*: é a versão norte-americana de IDEA, da *Caseware*-IDEA, que desenvolve consultoria e dá suporte sobre o produto.

d) Galileo: é um *software* integrado de gestão de auditoria. Inclui gestão de riscos de auditoria, documentação e emissão de relatórios para auditoria interna.
e) Pentana: *software* de planejamento estratégico de auditoria, sistema de planejamento e monitoramento de recursos, controle de horas, registro de *checklist* e programas de auditoria, inclusive de desenho e gerenciamento de plano de ação.

FONTE: Imoniana (2011, p. 55)

As vantagens destes *softwares* generalistas, segundo Imoniana (2011, p. 56) são:

a) O *software* pode processar vários arquivos ao mesmo tempo.
b) Pode processar vários tipos de arquivos com formatos diferentes. Por exemplo: EBCDIC ou ASCII.
c) Possibilidade de fazer integração sistêmica com vários tipos de *software* e *hardware*.
d) Reduz a dependência de o auditor ser especialista de informática para desenvolver aplicativos específicos que têm caráter generalista para todos os auditores de tecnologia de informação.

E as desvantagens são:

a) Como processamento das aplicações envolve gravação de dados (arquivos) em separado para ser analisada em ambientes distintos, poucas aplicações poderiam ser feitas em ambiente *on-line*.
b) Se o auditor precisar rodar cálculos complexos, o *software* não poderá dar este apoio, pois tal sistema, para dar assistência generalista a todos os auditores, evita aprofundar as lógicas e matemáticas muito complexas, principalmente da área de seguros e arrendamento mercantis.

8.2 *SOFTWARE* ESPECIALIZADO DE TI

Segundo Imoniana (2011, p. 56), "consiste no programa desenvolvido especificamente para executar tarefas numa circunstância definida. O programa pode ser desenvolvido pelo próprio auditor, pelo especialista da empresa auditada ou pelo terceiro contratado pelo auditor".

Ainda segundo Imoniana (2001, p. 56), as vantagens destes *softwares* são:

a) Pode ser interessante para atender aos sistemas ou às transações incomuns que não têm contemplados nos *softwares* generalistas. Por exemplo: *leasing*, cartão de crédito, crédito imobiliário, entre outros;

b) O auditor, quando consegue desenvolver *softwares* específicos numa área muito complexa, pode utilizar isso como vantagem competitiva.

As desvantagens destes *softwares* são:

a) Pode ser muito caro, uma vez que seu uso será limitado e normalmente restrito somente a um cliente;
b) A atualização deste *software* pode ser problemática por falta de recursos que acompanhem as novas tecnologias.

8.3 PROGRAMAS UTILITÁRIOS

O auditor utiliza os *softwares* utilitários para executar algumas funções muito comuns de processamento. Por exemplo: sortear arquivo, sumarizar, concatenar, gerar relatórios. Geralmente, os bancos de dados SQL, DBase 2 etc., possuem esses recursos. Para Imoniana (2011, p. 57), "vale ressaltar que esses programas não foram desenvolvidos para executar as funções de auditoria, portanto, não têm recurso tais como verificação de totais de controles ou gravação das trilhas de auditoria".

As vantagens destes programas utilitários, de acordo com Imoniana (2011, p. 57), são:

a) Pode ser utilizado como quebra-galho na ausência de outros recursos.

E as desvantagens são:

a) Sempre necessitará do auxílio do funcionário da empresa auditada para operar a ferramenta.

9 TÉCNICAS DE AUDITORIA DA TI

Para a execução de trabalhos, na fase de validação dos Pontos de Controle, há necessidade de conhecimento da tecnologia de computação e da forma como aplicar essa tecnologia para a verificação do sistema/ambiente computacional, segundo o conceito de controle interno (GIL, 2000, p. 67).

Segundo Gil (2000, p. 67), "as técnicas de computação são aplicadas tanto em nível de análise de sistemas quanto de programação, ou seja, o leque de tecnologia necessária ao auditor de sistemas é amplo".

Para Imoniana (2011, p. 57), as variadas metodologias podem ser chamadas de técnicas. Elas proporcionam aos usuários várias vantagens. São elas:

- Produtividade
  • Com a melhoria no processo de planejamento, ajuda na redução do ciclo operacional de auditoria, focalizando o exercício nas funções mais importantes. Ainda com algumas tarefas repetitivas sendo eliminadas evitam o estresse do auditor.
- Custo
  • Reduz custos relacionados com auditoria, pois não necessita de geração de relatórios e listagens para análise. Adicionalmente, o auditor tem acesso remotamente, eliminando a necessidade de deslocamento e poupando custo de viagens. Evita também o gasto referente ao desenvolvimento de programas pelas firmas de auditoria com a disponibilidade de *softwares* generalistas.
- Qualidade assegurada
  • Com o uso de *softwares* que têm padrões devidamente testados, o auditor aproveita para adequar seus trabalhos aos padrões internacionais geralmente aceitos obrigatoriamente, aumentando a qualidade dos serviços prestados. Ademais, 100% dos dados podem ser testados, consequentemente, aumentando a cobertura dos riscos de auditoria.
- Valor agregado
  • Disponibiliza tempestivamente resultados para a tomada de decisões que necessitam de mudanças de rumos mais urgentes, facilitando a correção também dos desvios ou irregularidades em tempo hábil. Ainda, possibilita a execução do procedimento analítico e sintético das contas e subcontas das demonstrações financeiras, preparação dos papéis de trabalho, possibilitando reflexão sobre impactos em âmbito global.
- Benefícios corporativos
  • Proporcionam às empresas de auditoria os seguintes benefícios:
- Eficiência nos trabalhos.
- Eficácia em termos de execução, de somente aqueles passos que atenuam riscos aparentes.
- Otimização dos recursos disponíveis principalmente a respeito de compartilhamento de ambientes entre vários auditores em múltiplas localidades.
- Melhoria na imagem do auditor, por utilizar tecnologia mais apropriada.
- Benefícios para o auditor
  • Proporcionam aos auditores os seguintes benefícios:
- Independência, pois não dependerá do auditor ou do seu funcionário de processamento de dados para gerar relatórios.
- Renovação do foco de auditoria, visando atender às expectativas e tendências do mercado.
- Eliminação das tarefas mais repetitivas, que geralmente podem ser automatizadas.
- Mais tempo para pensar e ser criativo nas sugestões para seus clientes, visto que o processo de emissão de relatórios costuma ser muito corriqueiro.
- Redução do risco de auditoria, uma vez que, tudo sendo programado, nada passará despercebido.

9.1 QUESTIONÁRIO

"Corresponde à elaboração de um conjunto de perguntas com o objetivo de verificação de determinado ponto de controle do ambiente computacional". (GIL, 2000, p. 78).

Essas questões, segundo Gil (2000, p. 78), "buscam verificar a adequacidade do ponto de controle aos parâmetros do controle interno (segurança lógica, segurança física, obediência à legislação, eficácia, eficiência etc.)".

Para Gil (2000, p. 78), existem dois aspectos que são críticos na aplicação da técnica questionário:

- Característica do ponto de controle.
- Momento histórico empresarial ou objetivos da verificação do ponto de controle.

De acordo com Gil (2000, p. 78), "os objetivos de verificação do ponto de controle vão determinar a ênfase a ser dada ao parâmetro do controle interno".

"As características do ponto de controle têm agregada a natureza da tecnologia computacional e o correspondente perfil técnico do auditor que irá aplicar o questionário". (GIL, 2000, p. 79).

Dessa forma, segundo Gil (2000, p. 79), podem-se ter questionários voltados para pontos de controles cujas perguntas guardarão características intrínsecas referentes à:

a) Segurança em redes de computadores
   - Segurança física dos equipamentos computacionais.
   - Segurança lógica e confidencialidade do *software*/informações que trafegam nos canais de comunicação.

b) Segurança do centro de computação
   - Controle de acesso físico e lógico às instalações de processamento de dados.
   - Segurança ambiental no tocante à infraestrutura de combate a incêndio, para enfrentar inundação, contra atentados e sabotagem, em situações de greve etc.

c) Eficiência no uso dos recursos computacionais
   - Tempo médio de resposta em terminal.
   - Tempo de uso dos equipamentos a cada dia.
   - Quantidade de rotinas catalogadas existentes.

d) Eficácia de sistemas aplicativos
   - Quantidades de informação geradas pelo computador e consumidas pelos usuários.

- Prazo de atendimento de novos sistemas, aos usuários.
- Tempo médio de solução dos problemas dos usuários da rede de computação, provida pelo *help-desk*.

A técnica questionário é, normalmente, aplicada de forma casada a outras técnicas de auditoria como entrevistas, visita *in loco* etc. Entretanto, conforme Gil (2000, p. 79), "o questionário pode ser aplicado a distância, ou seja, pode ser enviado ao auditado, respondido e analisado pelo auditor centralizadamente".

Segundo Gil (2000, p. 79), "esta abordagem permite ao auditor varrer um amplo universo de auditados". Particularmente, em ambiente de microinformática, devido à quantidade, à intensidade de dispersão dos equipamentos e à quantidade de usuários por equipamento a aplicação de questionários a distância permite uma auditagem constante com menor número de auditores.

Para Gil (2000, p. 80), esta auditoria básica via aplicação de questionários a distância possibilita o diagnóstico de pontos relevantes que possam ser auditados em maior nível de detalhamento em momento posterior no processo de arbitragem.

Ainda segundo Gil (2000, p. 80), "um inconveniente da abordagem aplicação de questionários a distância é a possibilidade de interpretações subjetivas tanto para questões quanto para respostas".

9.2 SIMULAÇÃO DE DADOS

É a técnica por excelência aplicada para teste de processos computacionais. Para Gil (2000, p. 81), "corresponde à elaboração de um conjunto de dados de teste a ser submetido ao programa de computador ou a determinada rotina que o compõe, que necessita ser verificada em sua lógica de processamento".

Segundo Gil (2000, p. 81), os dados simulados de teste necessitam prever situações corretas e situações incorretas de natureza:

- Transações com campos inválidos.
- Transações com valores ou quantidades nos limites de tabelas de cálculos.
- Transações incompletas.
- Transações incompatíveis.
- Transações em duplicidade.

Gil (2000, p. 82) afirma que a mecânica de aplicação do *test-check* implica as etapas:

1. Compreensão do módulo do sistema a ser avaliado/identificação de programas e arquivos.
2. Simulação de dados de teste pertinentes. Este momento impõe o alcance do parâmetro do controle interno e objetivado.
3. Elaboração dos formulários de controle do teste.
4. Transcrição dos dados de teste para um meio aceito pelo computador. Uma opção do auditor de sistemas é copiar partes do arquivo real de entrada no programa e fazer, via programa de computador, as alterações desejadas para alimentação da simulação de dados necessários.
5. Preparação do ambiente necessário para execução do teste. Criação de comandos de operação do programa de computador sob auditoria. Alimentação dos arquivos de dados simulados, com *labels* e códigos específicos desses arquivos de teste de auditoria.
6. Processamento dos dados de teste com utilização do programa real que contém as rotinas do sistema sob auditoria a serem validadas.
7. Avaliação dos resultados do teste via análise das listagens obtidas a partir do arquivo magnético gerado.
8. Emissão de opinião acerca do ponto de controle processo computadorizado (rotina ou programa) com a elaboração da documentação, ou seja, papéis de trabalho referentes à simulação de dados realizada.

9.3 VISITA *IN LOCO*

Corresponde à atuação pessoal do auditor junto a sistemas, procedimentos e instalações do ambiente computadorizado (GIL 2000).

Normalmente, segundo Gil (2000), essa técnica é combinada com outras técnicas de auditoria de computador, particularmente questionário, a visita *in loco* implica o cumprimento da seguinte sequência de procedimentos:

a) Marcar data e hora com a pessoa responsável que irá acompanhar as verificações, ou convocá-la no momento da verificação quando o fator surpresa se tornar necessário;
b) Anotar procedimentos e acontecimentos, coletar documentos, caracterizar graficamente a situação via elaboração de fluxo de rotinas e de *layout* de instalações.
c) Anotar nomes completos das pessoas e a data e hora das visitas realizadas.
d) Analisar os papéis de trabalho obtidos, avaliar respostas e a situação identificada.
e) Emitir opinião via relatório de fraquezas de controle interno.

Para Gil (2000, p. 86), "a presença do auditor é fundamental para a constatação física da existência de ativos computacionais da empresa, bem como seu estado de conservação e qualidade dos procedimentos de utilização".

9.4 MAPEAMENTO ESTATÍSTICO DE PROGRAMAS

De acordo com Gil (2000, p. 87), a técnica de computação que pode ser utilizada pelo auditor para efetuar verificações durante o processamento dos programas, flagrando situações como:

- Rotinas não utilizadas.
- Quantidades de vezes que cada rotina foi utilizada quando submetida a processamento de uma quantidade de dados.

Segundo Gil (2000, p. 87), a análise dos relatórios emitidos pela aplicação do mapeamento estatístico permite a constatação de situações:

- Rotinas inexistentes em programas já desativadas ou de uso esporádico.
- Rotinas mais utilizadas, normalmente, a cada processamento do programa.
- Rotinas fraudulentas e de uso em situações irregulares.
- Rotinas de controle acionadas a cada processamento.

Para a utilização desta técnica, Gil (2000) indica que há necessidade de ser processado um *software* de apoio em conjugação com o processamento do sistema aplicativo, ou rotinas específicas deverão estar embutidas no sistema operacional utilizado.

9.5 RASTREAMENTO DE PROGRAMAS

"Técnica que possibilita seguir o caminho de uma transação durante o processamento do programa". (GIL, 2000, p. 87).

Para Gil (2000, p. 88), "quando o teste de alimentação de determinada transação a um programa é realizado, pode-se identificar as inadequações e ineficiência na lógica de um programa. Esta abordagem, como consequência, viabiliza a identificação de rotinas fraudulentas, pela alimentação de transações particulares".

9.6 ENTREVISTA

Segundo Gil (2000, p. 88), "este método corresponde à realização de reunião entre o auditor e os auditados – profissionais usuários e de computação envolvidos com o ambiente ou o sistema de informação computadoriza sob auditoria".

Para Gil (2000, p. 88), a sequência de procedimentos correspondente a essa técnica são:

a) Analisar o ponto de controle e planejar a reunião com os profissionais envolvidos.
b) Elaborar um questionário para realização da entrevista.
c) Realização da reunião, com aplicação do questionário e anotação das respostas e comentários dos entrevistados a cada questão efetuada.
d) Elaboração de uma ata de reunião com o registro dos principais pontos discutidos a cada questão apresentada.
e) Análise das respostas e formação de opinião acerca do nível de controle interno do ponto de controle.
f) Emissão do relatório de fraquezas de controle interno.

"A técnica de entrevistas é frequentemente casada com outras técnicas de auditoria, visita *in loco*, aplicação de questionários, *test-desk* etc." (GIL, 2000, p. 89).

9.7 ANÁLISE DE TELAS E RELATÓRIOS

Segundo Gil (2000, p. 89), implica a análise de documentos, relatórios e telas do sistema sob auditoria no tocante a:

- Nível de utilização pelo usuário.
- Esquema de distribuição e número de vias emitido.
- Grau de confidencialidade de seu conteúdo.
- Forma de utilização e integração entre relatórios/telas/documentos.
- Distribuição das informações segundo o *layout* vigente.

A mecânica de aplicação da técnica, de acordo com Gil (2000, p. 89), implica o cumprimento das seguintes etapas:

a) Relacionar por usuário todos os relatórios/telas/documentos que pertençam ao ponto de controle a ser analisado.
b) Obtenção de modelo ou cópia de cada relatório/documento/tela para compor a pasta de papéis de trabalho.
c) Elaborar um questionário para a realização dos levantamentos acerca dos relatórios/telas/documentos.

d) Marcar antecipadamente a data e hora com as pessoas que fornecerão opinião acerca dos relatórios.
e) Realizar as entrevistas e anotar as observações e comentários dos usuários.
f) Analisar as respostas, formar e emitir opinião acerca do nível de controle interno.

Na utilização desta técnica, segundo Gil (2000, p. 90), é possível encontrar as seguintes principais fraquezas:

- Relatórios/telas/documentos não mais utilizados;
- *Layout* inadequado;
- Distribuição indevida de vias;
- Confidencialidade não estabelecida ou não respeitada.

As conclusões do trabalho, frequentemente, de acordo com Gil (2000, p. 90), "possibilitam reduzir os custos com a desativação parcial ou total de relatórios/telas/documentos".

"Esta técnica é primordial para avaliação do parâmetro eficácia do sistema". (GIL, 2000, p. 90).

9.8 SIMULAÇÃO PARALELA

Conforme Gil (2000, p. 90), "esta técnica consiste na elaboração de um programa de computador para simular as funções de rotina do sistema sob auditoria. Esta técnica utiliza-se dos dados rotineiros alimentados à rotina do sistema sob auditoria como entrada do programa de computador para auditoria, simulado e elaborado pelo auditor".

Enquanto na técnica de *test-desk* é simular dados e os submeter ao programa de computador que, normalmente, é processado na produção, Gil (2000, p. 90) "afirma que na simulação paralela simulamos o programa e submetemos ao mesmo os dados que foram alimentados ao programa em processamento manual".

A estrutura de aplicação desta técnica, segundo Gil (2000) é a seguinte:

a) Levantamento e identificação via documentação do sistema, da rotina a ser auditada e os respectivos arquivos de dados trabalhados.
b) Elaboração de programa de computador com a lógica da rotina a ser auditada. Compilação e teste deste programa irá simular em paralelo a lógica do programa de computador.
c) Preparação do ambiente de computação para processamento do programa de computador elaborado pelo auditor.

9.9 ANÁLISE DE *LOG/ACCOUNTING*

O *Log/Accounting* é um arquivo, gerado por uma rotina componente do sistema operacional, que contém registros do *hardware* e do *software* que compõem um ambiente computacional.

A tabulação deste arquivo *Log/Accounting* permite a verificação da intensidade de uso dos dispositivos componentes de uma configuração ou rede de computadores, bem como o uso do *software* aplicativo e de apoio vigente.

Tanto a rotina quanto o correspondente arquivo de *Log/Accounting* foram desenvolvidos para serem usados pelo pessoal da computação. Entretanto, representam também, uma excelente ferramenta para a auditoria de sistemas para:

- Identificação de ineficiência, no uso do computador.
- Apuração do desbalanceamento da configuração do computador, pela caracterização de dispositivos que estão com folga ou sobrecarregados.
- Determinação dos erros de programas ou de operação do computador.
- Flagrar uso de programas fraudulentos ou utilização indevida do computador.
- Captar tentativas de acesso a arquivos indevidos, ou seja, senhas/*passwords* não autorizados.

Deve haver na área da computação, profissionais responsáveis pela análise do uso do computador e o trabalho desses profissionais precisa ser auditado, através da análise dos registros históricos e dos relatórios por eles produzidos.

O trabalho da área de computação sobre o *Log/Accounting* deve gerar Indicadores da Qualidade (IQ) do monitoramento do computador, bem como estudos e planejamento de capacidade da configuração/rede de equipamentos, com a finalidade de obter maior rendimento do parque computacional dentro de um nível de segurança adequado.

FONTE: Gil (2000, p. 91)

Para Gil (2000, p. 93), "a observação crítica da qualidade da análise do *Log/Accounting* e a discussão dos dados obtidos, com a aplicação da mecânica pessoal de computação, em dado intervalo de tempo, e a consequente conclusão da adequacidade ou não da utilização de *hardware* e de *software* é a tarefa do auditor de sistemas".

A técnica de auditoria análise do *Log/Accounting* é um poderoso instrumento de auditoria, porém sua aplicação requer grande conhecimento de computação. Uma de suas aplicações é identificar o uso de programas fraudulentos ou não pertencentes à empresa. Segundo Gil (2000, p. 93), "neste caso, uma série de análises complementares precisam ser feitas para a constatação da irregularidade".

9.10 ANÁLISE DO PROGRAMA-FONTE

Esta técnica, de acordo com Gil (2000, p. 94), "implica a análise visual do código-fonte (linguagem em que o usuário ou programador escreve o programa) do programa de computador componente do sistema sob auditoria".

O auditor de sistemas necessita assegurar-se de que está testando a versão correta do programa que "rodou" ou irá "rodar". Para tal, segundo Gil (2000, p. 94), "o auditor compara o *label* do programa-fonte gravado na biblioteca-fonte com o *label* do programa-objeto gravado na biblioteca-objeto (onde os programas estão em linguagem de máquina, ou seja, módulo de carga executável)".

O auditor pode, conforme Gil (2000), ainda, para maior certeza de que verifica as instruções que efetivamente compõem o programa em linguagem de máquinas, executar os seguintes procedimentos:

a) Preencher uma Ordem de Serviço determinando à produção que compile o módulo-fonte que se encontra na biblioteca-fonte.
b) Executar um *software* específico que compare o código-objeto gerado em *a*, com o código-objeto do programa que se encontra gravado na biblioteca-objeto da produção.
c) Efetuar verificações em eventuais divergências que ocorram em *b*.

"É importante ressaltar que esta técnica exige profundos conhecimentos de processamento eletrônico de dados por parte do auditor de sistemas". (GIL, 2000, p. 95).

9.11 *SNAPSHOT*

Técnica que fornece uma listagem ou gravação do conteúdo das variáveis do programa (acumuladores, chaves, áreas de armazenamento) quando determinado registro está sendo processado. Para Gil (2000, p. 95), "a quantidade de situações a serem extraídas é predeterminada".

Essa técnica, segundo Gil (2000) corresponde na realidade a um *dump* parcial da memória, basicamente, das áreas de dados.

"À semelhança do *mapping* e do *tracing*, necessita de um *software* especial "rodando" junto com o programa aplicativo, ou que as características *SNAPSHOT* estejam embutidas no sistema operacional". (GIL 2000, p. 95).

De acordo com Gil (2000, p. 95), "esta é uma técnica usada como auxílio à depuração de programas, quando há problemas e realmente exige fortes conhecimentos de processamento eletrônico de dados por parte do auditor de sistemas".

RESUMO DO TÓPICO 1

Caro(a) acadêmico(a)! Neste tópico, você estudou que:

- Todo sistema está sujeito a falhas, erros e mal uso de recursos em geral. Tanto o computador como a mente humana são instrumentos para grandes realizações, porém não são infalíveis.

- A filosofia da auditoria de tecnologia de informação está calcada em confiança e em controles internos.

- Dependendo da sofisticação do sistema computadorizado e considerando as características do auditor de tecnologia de informações, poderá ser usado para auditar qualquer uma das três abordagens: ao redor do computador, através do computador e com o computador.

- Auditoria ao redor do computador no passado era uma abordagem muito solicitada pelos auditores, devido ao não envolvimento de muita tecnologia de informação.

- O uso da auditoria através do computador envolve mais do que mera confrontação de documentos-fonte com os resultados esperados, uma vez que os sistemas têm evoluído muito.

- A atividade de planejamento em auditoria de sistemas de informações é imprescindível para melhor orientar o desenvolvimento dos trabalhos.

- A fim de garantir a evolução e o aprimoramento técnico dos profissionais da equipe de auditoria de TI, deve-se avaliar o desempenho, elogiando os pontos fortes do auditor, auxiliar no reconhecimento das fraquezas e na elaboração de um plano para superá-las para que se desenvolva um profissional qualificado e consciente.

- A avaliação dos procedimentos de controles internos em ambientes de sistemas de informações de uma organização é um trabalho executado pelo auditor que tenha habilidade em tecnologia de informações.

- Em qualquer sistema de informação complexo ou moderado, sua avaliação pelos auditores internos se processa através do uso de ferramentas adequadas de auditoria, métodos e técnicas.

AUTOATIVIDADE

1 Cite três objetivos de um sistema geral de Controle Interno.

2 Quais são as estratégias normalmente adotadas para constituir uma equipe de auditoria de TI?

3 Quais são as três abordagens de auditoria de sistemas de informações?

4 Cite três vantagens proporcionadas pelas técnicas de auditoria.

5 Comente sobre duas técnicas de auditoria que você utilizaria e o motivo.

Assista ao vídeo de resolução da questão 1

TÓPICO 2

TIPOS DE AUDITORIAS

1 INTRODUÇÃO

Caro(a) acadêmico(a)! Neste tópico será possível conhecer alguns tipos de auditoria. São os seguintes: auditoria de controles organizacionais; de aquisição, desenvolvimento e manutenção de sistemas; de controle de *hardwares*, acesso e de suporte técnico; de operação do computador; procedimentos de auditoria de sistemas aplicativos; auditoria de planos de segurança e redes e relatórios de auditoria.

2 AUDITORIA DE CONTROLES ORGANIZACIONAIS

Os controles organizacionais e operacionais são os controles instalados nos processos de fluxo das transações econômicas e financeiras dos sistemas de informações, auxiliando-os na consecução dos objetivos dos negócios. Para Imoniana (2011, p. 76), "a efetividade deste controle depende da experiência organizacional dos gestores, uma vez que exige demonstração de práticas e habilidades gerenciais". Poucas são as interferências e as influências externas que afetam a implementação dos controles.

A responsabilidade de controles organizacionais repousa, segundo Imoniana (2011), nas seguintes tarefas:

- Delineamento das responsabilidades operacionais.
- Coordenação de orçamento do capital de informática e bases.
- Desenvolvimento e implementação das políticas globais de informática.
- Intermediação com terceiros (*networking*).
- Gerenciamento de suprimentos.
- Desenvolvimento de plano de capacitação.

Os gestores, na medida do possível, tentam delinear as funções para, em primeiro lugar, identificar responsabilidades para todas as tarefas realizadas na organização e, em segundo lugar, amenizar conflitos que certamente surgirão no decorrer do dia a dia operacional. Para Imoniana (2011, p. 77),

> esse desmembramento das atividades é caracterizado por agregação das funções incompatíveis e é uma medida de controle para enfatizar o evangelho de responsabilidades, fazendo com que cada um seja cobrado por suas tarefas de acordo com seus resultados. Esse controle geral é vital tanto no ambiente manual como no ambiente computadorizado. Entretanto, a segregação de funções (autorização, gravação e acesso para ativos) pode não ser efetivamente possível em um ambiente de computador.

Para que os controles organizacionais sejam efetivos, deve haver lealdade e confiança mútua entre a empresa e os funcionários. Os funcionários devem ser tratados com respeito, justiça e, sobretudo, honestidade; deve-se fazer com que eles percebam que assim é cultura da empresa, evitando-se percepção da falta de motivação que fomenta ingerência. Salários baixos e condições subumanas de trabalho podem propiciar o descumprimento dos controles organizacionais da área de informática que, normalmente, devido à natureza das atividades, tem acesso privilegiado às informações estratégicas da empresa (IMONIANA, 2011).

Embora exista ambiente complexo de computação que acompanhe todas as tendências de tecnologia de informação de que o estabelecimento precisa, isto por si não garante segurança se as políticas organizacionais e operacionais não forem implementadas com rigor. Imoniana (2011) diz que no ambiente de alta tecnologia, quando segregamos as funções, apenas dificultamos a propensão para fraudes dos fluxos operacionais. Portanto, os ciclos operacionais, que têm tarefas de originar as transações e as autorizações segregadas, para que ocorra fraude, necessitariam de conivências de mais de duas pessoas, ao invés de concentrar todo o ciclo de transações críticas na mão de apenas uma. Deve-se ressaltar que os usuários finais apenas precisam de acesso aos dados, aplicações e funções para atender somente a suas atribuições de tarefas e nada mais.

Entretanto, para que os objetivos administrativos sejam alcançados, é imprescindível, conforme Imoniana (2011, p. 77),

> estabelecer claramente as políticas de tecnologia de informações e, a partir dessas, cabe aos gerentes traduzir isso em linguagem operacional através de procedimentos administrativos, detalhando inclusive as definições e os princípios, evitando-se dupla interpretação. De acordo com ênfases dadas pela organização, sistemas e métodos, cada procedimento administrativo deve descrever quais são as entradas do ciclo operacional, o processamento a ser feito e os resultados que este deverá proporcionar ao próximo ciclo.

3 AUDITORIA DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

As funções de aquisição, desenvolvimento, manutenção e documentação de sistemas são atribuídas aos indivíduos que têm competências para conceber e implantar sistemas. Conforme Imoniana (2011, p. 92), "isso é feito naturalmente junto com os usuários com o propósito de atender aos objetivos dos negócios e, assim, cumprir obrigações da área de desenvolvimento de sistemas e garantir também as funções de pós-implantação de sistemas".

De forma analítica, segundo Imoniana (2011, p. 92), as funções de aquisição, desenvolvimento, manutenção e documentação de sistemas incluem:

- Planejamento de sistemas de informações.
- Aquisição de sistemas.
- Especificação, programação, teste e implementação de sistemas novos.
- Modificação dos programas das aplicações existentes.
- Manutenção preventiva dos sistemas aplicativos.
- Documentação e controle sobre versões de programas em produção.

A função de desenvolvimento bem controlada tem procedimentos estabelecidos para a aquisição e o desenvolvimento de novos sistemas. Também permitem alteração dos sistemas existentes, inclusive teste e documentação de sistemas novos. Para Imoniana (2011, p. 92), "Quando os usuários não estão familiarizados com operação de um sistema novo ou com os relatórios, encontrarão dúvidas frequentes de processamento ou dificuldades para sugestão de modificações nos sistemas que podem ter deficiências significativas no seu controle".

Normalmente, quando novos sistemas ou modificações significativas nos sistemas existentes são implementados, o risco de erros relacionados a transações processadas por esses sistemas pode ser aumentado. Para tais sistemas que não possuam histórico de confiança ou precisão no seu processamento para suportar um ceticismo sobre existência de risco, o usuário preocupa-se com relação onde efetivamente estão ocorrendo as modificações promovidas nos sistemas. Consequentemente, quando novos sistemas ou sistemas que sofreram mudanças significativas são auditados como parte dos trabalhos definidos nos planejamentos de auditoria de uma empresa, pode-se desejar rever controles sobre a aquisição, o desenvolvimento e a modificação de sistemas atentando para seu impacto sobre negócios (IMONIANA, 2011).

3.1 CONTROLES DE DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

O desenvolvimento efetivo de um sistema requer participação da alta cúpula da administração. Para Imoniana (2011, p. 93), "isso pode ser alcançado por um comitê de direção composto de representantes de alto nível de usuários de sistemas. O comitê aprova ou recomenda alterações nos projetos e revisa o progresso deles".

Imoniana (2011) afirma que, para desenvolver um sistema, deve-se promover o estudo de viabilidade econômica, operacional e técnica de aplicações novas necessariamente requerendo avaliações e também propondo sistemas.

Imoniana (2011) também afirma que outro controle necessário nessa fase é o estabelecimento de padrões para sistema. Esses padrões são cumpridos pelos usuários ao preencher os requerimentos de sistema e determinados durante a análise de sistemas.

"De acordo com as tendências e o lapso do tempo, as mudanças naturalmente ocorrerão; essas mudanças nos sistemas deveriam estar sujeitas a controles rígidos". (IMONIANA, 2011, p. 93).

O armazenamento de programas é um fator que garante a continuidade das operações. Para Imoniana (2011, p. 94), "devem ser armazenadas versões de programas de aplicação crítica em código de objeto".

Para assegurar a aderência aos propósitos dos sistemas em desenvolvimento, durante seu teste, deveriam ser testados não só programas propostos com dados incorretos ou incompletos, como também dados tipicamente errados para determinar se foram implementados controles corretos nos sistemas. Segundo Imoniana (2011, p. 94), "os dados de teste deveriam testar todas as funções do sistema, inclusive as capacidades de edições e consistência de dados. A função de edição inclui sucessão de diálogos que confere, valida e testa a racionalidade de dados".

A fim de evitar o uso de *softwares* piratas, que resultem em contingência legal, devem ser implementados também controles que previnam o uso de *software* sem licença no domínio público e da empresa em geral. Normalmente, *software* com as devidas licenças estabelecem um número mínimo ou em alguns casos ilimitado de cópias permitidas de *software* em determinados locais, máquinas particulares ou redes em unidade ou em toda a companhia, se o uso for livre. Segundo Imoniana

(2011, p. 94), "o acordo pode restringir reprodução ou revenda, e pode prover apoio para subsequente melhoria do produto". Assim, uma brecha do acordo de licenciamento ou o uso de *software* sem licença pode expor uma companhia a risco. Consequentemente, deveriam ser desenvolvidas políticas de *software* para a companhia, e os usuários deveriam estar atentos às consequências negativas de violar essas políticas, e deveriam ser ministrados, inventariados periodicamente para determinar se *software* sem licença está em uso.

3.2 CONTROLES DE DOCUMENTAÇÃO DE SISTEMAS

A documentação é um conjunto de artefatos que apoiam, explicam e descrevem a aplicação dos programas. Existem documentações próprias para cada momento do processo de *software*, ou seja, antes das implementações, durante a execução do projeto de implementação e depois. Esta documentação do após, é destina para auxiliar no uso dos *softwares*, com objetivo de orientação sobre o funcionamento destes sistemas. Segundo Imoniana (2011, p. 95), "é útil não só para os próprios analistas de sistemas como também para os usuários, controle pessoal, empregados novos, auditores, programadores, entre outros, que desejam conhecer o funcionamento de sistemas". Entre os padrões necessários para uma boa documentação, estão as seguintes:

a) Documentação deveria ser guardada em uma biblioteca que tenha um controle de acesso.
b) Documentação deveria estar sujeita a padrões uniformes relativos a técnicas de *flowcharting*, codificação e procedimentos de modificação (incluindo própria autorização).
c) Documentação de sistema inclui narrativas, *flowcharts*, que a definição de sistema usou para seu desenvolvimento, contribuição e formas de produção, arquivo e planos de registro, controles, autorizações de mudança e procedimentos posteriores.
d) Documentação de programas contém descrição, *flowcharts* de programa e mesas de decisão, listings de programa de fonte, dados de teste, contribuição e produção, arquivos detalhados e planos de registro, pedidos de mudança, instruções de operador e controles.
e) Documentação operacional (manual de operação do computador) provê informação sobre organização, arquivos necessários e dispositivos, procedimentos de contribuição, mensagens do console e ações de operador responsável, tempos necessários, procedimentos de recuperação, disposição de produção e controles.
f) Documentação processual inclui o plano-mestre do sistema e operações a serem executados, padrões de documentação, procedimentos para controlar arquivos e padrões para análise de sistemas, programação, operações, segurança e definição de dados.
g) Documentação de usuário descreve o sistema e procedimentos para entrada de dados, conferência e correção de erros, formatos e usos de relatórios.

FONTE: Imoniana (2011, p. 95)

3.3 OBJETIVOS DA AUDITORIA

Para Imoniana (2011, p. 95), as seguintes questões referentes aos objetivos de auditoria de controle de aquisição, desenvolvimento, manutenção e documentação de sistemas aplicativos devem ser respondidas:

- Há procedimento de formalização da real necessidade para um novo sistema?
- As especificações são feitas de forma diligente, confrontando os conhecimentos dos usuários com os de analista de sistema, visando dar suporte aos projetos?
- Os desenvolvimentos de testes e instalação na produção são feitos sem traumas para os usuários?
- Há informações apresentadas para que os usuários possam decidir entre aquisição e desenvolvimento interno?
- O desenvolvimento segue os padrões e utiliza todas as ferramentas para alinhá-lo com os sistemas já existentes?
- As questões básicas operacionais/funcionalidade, tecnologia, pós-vendas, segurança e de análise de custo e benefícios, entre outras, são esclarecidas quando da decisão de compras externas?
- Os usuários são treinados para utilizar os sistemas com todos os potenciais que possuem?
- As manutenções são feitas sem interrupção das operações normais da empresa?
- As documentações são consistentes e disponíveis para orientar os usuários?

4 AUDITORIA DE CONTROLES DE *HARDWARE*

O controle de *hardware* objetiva implantar procedimentos de segurança física sobre os equipamentos instalados em ambiente de informática de uma organização. Aponta como os contatos físicos dos usuários aos variados recursos são controlados, além de auxiliar no monitoramento de seu uso adequado para agregar valor aos negócios (IMONIANA, 2011).

"As funções que possuem mecanismo adequando para restringir acessos de pessoas ao ambiente de computador são conhecidas por segurança física". (IMONIANA, 2011, p. 102).

O controle envolve aplicação do próprio equipamento para se proteger contra riscos estruturais, seja ele relacionado ao componente específico ou complexo e miniatura de unidade *palmtop*. Segundo Imoniana (2011, p. 102), "abrange também os controles referentes à proteção da vida de pessoas, além de unidades periféricas cuja manutenção limita-se a certos empregos-chave". Essa função evita perda de *hardwares* e os protege contra o não funcionamento que gera parada nas operações, que resulta na desvantagem competitiva e em perdas financeiras.

4.1 COMPREENSÃO DO PROCESSO DE CONTROLE DE *HARDWARES*

Para Imoniana (2011, p. 102), "os controles podem ser físicos e automatizados. Físicos implicam a diversidade de procedimentos que orientam o manuseio dos equipamentos, enquanto os controles automatizados representam os controles construídos junto com os equipamentos pelo fabricante, que ajudam a descobrir e controlar erros que surgem do uso do próprio equipamento".

O significado de controles de *hardware* para auditores é que eles asseguram a execução correta de instruções dadas para as máquinas através de programas representados pelos sistemas de aplicação. De acordo com Imoniana (2011, p. 103), "sem procedimentos de controles de *hardware*, auditores teriam dificuldades em levantar *modus operandi* dos *hardwares* que operam em ambiente de informática". Além de implementar os recursos preventivos, vale questionar se há recursos corretivos que evitam paradas bruscas, sem prejuízo aos *workflows* das transações empresariais.

Para que os controles de *hardware* sejam efetivos, é necessário fazer inventários de *hardwares*.

Segundo Imoniana (2011, p. 103), essa atividade é caracterizada pela verificação automática dos recursos construídos no *hardware* ou até adicionados ao próprio equipamento durante sua aplicação dia a dia. Inclui o diagnóstico de:

a) BIOS.
b) Processadores (*chips*).
c) Sistemas operacionais e linguagens.
d) Fabricante/modelo e séries.
e) Monitor e resolução.
f) Placas de *modem*, som, vídeo etc.

Ainda segundo Imoniana (2011, p. 103), "quando esta função é embutido no computador, com programação periódica, rotinas podem diagnosticar e conferir os problemas de *hardware* e permitir que o próprio sistema dê o aviso prévio sobre os problemas eminentes".

Imoniana (2011) afirma que a padronização dos modelos de equipamentos é um procedimento fundamental para auxiliar na implantação de controle efetivo. Caso a empresa decidir adquirir equipamentos diferentes, deve-se atentar para configurar de forma homogênea todas as estruturas dos *hardwares* operacionais.

Deve-se atentar para o risco de instalação de *softwares* piratas nos equipamentos da empresa. Para isso, as empresas devem implementar política de segurança abrangente que contemple penalidades para sua infringência. Todavia, Imoniana (2011, p. 103) afirma que existem recursos de auditoria que possibilitam descobrir *softwares* executáveis sem as devidas licenças, seja em ambiente *stand alone*, seja em ambiente de rede.

Segundo Imoniana (2011, p. 103),

> entre os recursos utilizados para amenizar os riscos de segurança no controle de *hardware* incluem-se: extintores de incêndio, *sprinklers*, gás halon etc. Com relação à restrição de pessoas externas, cabe ressaltar a importância de utilizar recursos tais como: *Trasnportable Access Keys*, *Firewalls* etc. Para certos extremos deve-se isolar totalmente o ambiente de computação.

Firewall é um recurso (*software* ou *hardware*) aplicado pelos administradores de segurança de rede para impedir acessos lógicos de fora para dentro do ambiente empresarial, para controlar os acessos de pessoas não autorizadas, e de dentro para fora, o controle e limitações de acesso à grande rede. De acordo com Imoniana (2011, p. 104), "ele atua como se estivesse constituindo um muro com painel de aço, por volta do ambiente de computação da empresa. Ele restringe acesso dos *hackers* e também limita extensão da infecção de vírus".

"Para que sejam evitadas paradas não previstas, aconselha-se implementar contratos de manutenção preventiva ou manter equipes de manutenção. A título de plano mais abrangente, deve-se implementar um plano de desastre, contingência e de recuperação de dados, testados periodicamente para garantir sua operacionalidade". (IMONIANA, 2011, p. 104).

"Sucateamento dos equipamentos obsoletos é questão importante a ser tratada, para atender a questões de meio ambiente e para manter os equipamentos renovados, atentando para desafios de tecnologia da informação". (IMONIANA, 2011, p. 104).

4.2 OBJETIVOS DA AUDITORIA DE CONTROLES DE *HARDWARES*

Segundo Imoniana (2011, p. 104), há dois eixos preocupantes quando se discute auditoria de controles de *hardwares*:

- Primeiro, no tocante aos equipamentos capazes de restringir acessos internamente dentro da organização, por consequência garantindo proteção de terminais, CPUs, servidores, unidades de conversão de dados, fitas, vidas etc.
- Segundo, se há equipamentos que restrinjam acessos físicos de pessoas alheias ao ambiente de processamento. Pessoas que têm interesse pelas informações da organização e que não têm permissão para acessá-las.

Para Gil (2000, p. 146), os seguintes aspectos devem ser validados pelo auditor de sistemas no que tange segurança física e ambiental:

a) Sistema de alimentação elétrica.
b) Controle de condições ambientais.
c) Segurança contra fogo e outros riscos.
d) Sistema de controle de acesso.
e) Localização de construção de um centro de computação.
f) Segurança dos recursos humanos.
g) Segurança dos recursos materiais.

5 AUDITORIA DE CONTROLES DE ACESSO

As atividades de controle de acesso lógico às informações, *softwares*, e dados são atribuídas à tarefa de desenvolvimento, implementação e acompanhamento de políticas de segurança de informações. Para Imoniana (2011, p. 114), "essa tarefa cabe ao administrador de segurança de informações, indivíduo que tem a responsabilidade de supervisionar a área de segurança das informações e implementar todas as políticas de controle de acessos".

Segurança de acesso lógico refere-se à proteção dada pelos recursos tecnológicos de um ambiente de sistema computadorizado contra acessos não autorizados aos dados ou informações não permitidas aos usuários específicos, com exceção do proprietário, ou seja, informações que não são públicas. Segundo Imoniana (2011, p.114), "normalmente, a regra de *need-to-know* é aplicada uma vez que somente aquele usuário que tenha necessidades operacionais terá acesso".

Para Gil (2000, p. 150), "a segurança lógica diz respeito à modificação dos recursos tecnológicos, informações e *software*, e a confidencialidade diz respeito à captação indevida desses mesmos recursos tecnológicos". Para a manutenção da segurança lógica e da confidencialidade é necessário validar e avaliar controles lógicos inseridos, bem como proteger informações e programas.

"O controle de segurança de acesso é feito com o auxílio de senhas, estabelecidas para cada usuário adequadamente identificado no sistema". (IMONIANA, 2011, p. 114).

Para Imoniana (2011, p. 114),

> o uso de senha números de identificação é um controle efetivo em um sistema *on-line* para prevenir acesso sem autorização a arquivos de sistemas. São mantidas tabelas de pessoas autorizadas no computador na qual deve haver uma confrontação quando requisitado acesso. A entrada de senhas ou números de identificação é um jogo pré-programado de perguntas pessoais que pode ter, além do uso de distintivos, cartões magnéticos ou leituras ópticas, outras formas como palma da mão, retina etc.

Ainda de acordo com Imoniana (2011, p. 115), "um cartão de segurança pode ser usado num sistema de forma que usuários tenham que alimentar sua ID e uma senha. A permissão dada para aquele usuário lhe privilegia acesso de registros quantas vezes quiser, mas atentando para suas características (data, tempo, duração etc.)".

Imoniana (2011) ainda afirma que a própria autenticação de usuário por meio de senha requer para tais procedimentos gerados para assegurar aquelas senhas são válidos e que só são conhecidos pelos próprios indivíduos. Assim, uma senha não deveria ser exibida quando é digitada num teclado, necessitando de uma máscara para esconder os caracteres digitados.

Ainda de acordo com Imoniana (2011, p. 114), "para ter eficácia no procedimento de controles de acesso lógico, recomenda-se adquirir e implantar *softwares* de segurança de informações, tais como: *Access Control Facility* (ACF2), *Top Secret*, *Resource Access Control Facility* (RACF) entre outras diversidades de *softwares* existentes no mercado". Estes devem ser customizados para atender às políticas de segurança de cada organização. A complexidade da customização dos parâmetros de segurança dependerá do nível de conscientização e uso de tecnologia de informação de cada ambiente.

Uma função de segurança bem controlada, segundo Imoniana (2011) tem mecanismos para restringir o acesso físico aos recursos de computação, programas

para restringir acesso lógico a esses recursos e procedimentos estabelecidos para monitorar e assegurar a segurança de informações. Perda de *hardware* ou meios físicos de arquivo de dados, alterações não autorizadas de dados ou programas, ou controles programados ineficientes, podem indicar ineficiência no controle da segurança de acessos lógicos.

Existem dois aspectos que são importantes para avaliação dos controles de acesso:

- Acesso físico – controle sobre o acesso físico ao *hardware*, incluindo a CPU, unidade de disco, terminais e arquivos de dados.
- Acesso lógico – controle sobre acessos aos recursos do sistema, incluindo a possibilidade de acesso aos dados ou ao processamento de programas e transações.

O controle de acesso pode ser particularmente importante em clientes com sistemas complexos que tenham numerosos controles programados ou executem autorizações automáticas e rotinas de aprovação para contabilizar transações como aprovações de pagamento. Segundo Imoniana (2011, p. 115), "o acesso aos sistemas computadorizados por pessoas desautorizadas pode afetar o processamento de dados, que resulta em erros e perda de ativos".

Para Imoniana (2011, p. 115), para execução de auditoria de acesso lógico, algumas perguntas devem ser feitas, incluindo as seguintes:

> a) A empresa possui rotinas de aprovação e autorização automática que podem causar a movimentação de grande quantidade de ativos, incluindo caixa, investimentos ou estoques?
> b) Um número significativo de procedimentos de controle programados depende da existência de controles de acesso adequados, isto é, de conhecimento dos proprietários dos sistemas?
> c) As competências exigidas dos funcionários são disponíveis no ambiente que o sistema operará?

6 AUDITORIA DE OPERAÇÃO DO COMPUTADOR

A operação do computador compreende função da área de informática que aciona *Inicial Program Loader* (*IPL*), os programas que ligam os computadores e também os desligam. Quando da ligação dos computadores, todos os recursos atualmente elencados nos *scripts* são acionados junto com o sistema operacional. Vale ressaltar que entre os itens que podem constar nos *scripts* estão todos os sistemas aplicativos ou sistemas de apoio à tomada de decisão que se deseja usar na consecução dos objetivos empresariais e os recursos periféricos que se deve usar (IMONIANA 2011).

O auditor necessita conhecer todas as operações e serviços disponibilizados pelos centros de processamento e documentar os controles organizacionais. Imoniana (2011, p. 125) destaca as operações mais comuns:

- Planejamento, controle e monitoramento das operações.
- Planejamento da capacidade.
- Monitoramento de todos os sistemas e as redes.
- Inicialização do sistema e do desligamento.
- Gravação, rastreamento dos problemas e monitoramento de tempo de respostas.
- Gerenciamento de mudanças estruturais e pessoais.
- Gestão das unidades, dos periféricos e inclusive dos equipamentos remotos.
- Gerenciamento de bibliotecas.
- Programação dos processamentos e acompanhamento das operações.
- Automação da produção.
- *Backup* de sistemas, programas, dados e banco de dados.
- Gerenciamento de *help desk*.
- Coordenação e programação de *upgrades* dos equipamentos.
- Gestão de *restart/recovery*.

Vale destacar que os controles exercidos em relação às mudanças que ocorrem em ambiente de processamento de dados que geralmente impactam significativamente nas operações do dia a dia da empresa devem ser tratados com bastante cuidado. Normalmente, para se fazer mudança é preciso estabelecer com as áreas e usuários os dois extremos, a saber: o momento crucial (pico das operações) e o momento de pouca movimentação e do uso reduzido do computador. De posse dessas informações, podem-se programar as modificações significativas sem causar impactos negativos ou atravancar as transações da empresa (IMONIANA, 2011).

6.1 OBJETIVOS DE AUDITORIA

De acordo com Imoniana (2011, p. 127), "o objetivo de auditoria dos processos operacionais de informática é garantir que todos os passos envolvidos na originação de dados, as lógicas envolvidas no processamento das tarefas e os procedimentos mínimos de emissão de relatórios sejam obedecidos".

Entretanto, o objetivo da auditoria de controles de operação de computadores tem como foco principal levantar a existência de controles que assegurem que as operações das transações econômicas e financeiras executadas na empresa sejam fidedignas. Ainda, segundo Imoniana (2011) visa confirmar o nível de confiabilidade dos auditores, das demonstrações financeiras ou auditoria interna neste ambiente.

6.2 PROCEDIMENTOS DE CONTROLES INTERNOS

De acordo com Imoniana (2011, p. 127),

> uma função de operação bem controlada tem procedimentos para assegurar que os *jobs* (serviços) sejam programados e processados adequadamente; consequentemente, relatórios e outros *outputs* (saídas ou relatórios) são distribuídos em tempo e de forma controlada, e os meios de arquivo de dados, inclusive *backups*, são adequadamente protegidos. Falhas frequentes dos sistemas, erros de processamento significativos e atrasos ou perdas de dados podem indicar a existência de deficiências significativas no controle de operação.

Procedimentos adequados de operação, quando executados consistentemente por pessoal competente, contribuem para a confiabilidade do processamento. Operação inadequada do computador pode causar processamentos incompletos, atrasados ou incorretos.

7 AUDITORIA DE CONTROLES DE SUPORTE TÉCNICO

A função de suporte refere-se aos usuários de tecnologia de informações e ao nome dos indivíduos com responsabilidade de implantar, manipular e supervisionar os recursos de alta tecnologia e de dar apoio à sua utilização nas empresas (IMONIANA, 2011).

As funções das atividades de suporte técnico podem ser separadas em dois blocos principais: as funções rotineiras e as funções esporádicas.

- Funções rotineiras:
  - Gerenciamento de *help desk*.
  - Socorro aos problemas de instalação de redes.
  - Monitoramento das ocorrências de problemas.
  - Treinamento dos usuários dos *softwares*.
  - Revisão preventiva dos equipamentos.
  - Substituição dos equipamentos antigos.
  - Segurança de informações quando não há administrador de segurança de informações.
- Funções esporádicas:
  - Dimensionamento do banco de dados.
  - Instalação de *softwares* utilitários.
  - Manutenção dos sistemas operacionais.
  - Instalação de *upgrades*.
  - Avaliação de *softwares* para fins de compras.
  - Padronização dos recursos de TI.
  - Ativação de redes (estações etc.).

FONTE: Imoniana (2011, p. 133)

7.1 COMPREENSÃO DO PROCESSO DE SUPORTE TÉCNICO

A compreensão do processo de suporte técnico, segundo Imoniana (2011) é de fundamental importância no decorrer das atividades de auditoria de sistemas para que possamos levantar todos os recursos existentes, níveis de complexidade, qualificação dos empregados, frequências de prestação de suporte para os usuários e as tendências empresariais em acompanhar os avanços de tecnologia de informações.

Imoniana (2011) afirma que uma função de suporte bem controlada tem procedimentos estabelecidos para a manutenção do sistema que controla o sistema operacional e outros recursos importantes, como o gerenciador de banco de dados e redes de comunicação. Falhas frequentes no sistema, tais como: incapacidades dos sistemas aplicativos de acessarem as transações *on-line*, para acessar o computador central, ou outros problemas genéricos que indicam desativação das capacidades de compartilhamento dos recursos de redes, tais como impressoras, entre outros, podem indicar a existência de deficiências no controle de suporte ao sistema de informações.

7.2 OBJETIVOS DE AUDITORIA

De acordo com Imoniana (2011, p. 134), "o objetivo de auditoria de suporte técnico é de constatar se os recursos de alta tecnologia da empresa estão sendo utilizados adequadamente. Ou seja, confirmar se os referidos recursos desenvolvidos e implementados estão contribuindo para o aumento de valor agregado ou ajudando a destruir o valor da empresa".

Ainda de acordo com Imoniana (2011, p. 134), "é importante ressaltar, às vezes, as empresas adquirem equipamentos de alta geração, *softwares* mais utilizados atualmente e equipes bastante qualificadas, mas devido à falta de cumprimento das obrigações de suporte técnico, os recursos não estão disponíveis quando são mais necessitados".

7.3 PROCEDIMENTOS DE CONTROLES INTERNOS

Segundo Imoniana (2011), geralmente, se tem maior dificuldade com a documentação dos procedimentos de controles de suporte técnico no processo de auditoria de sistemas de informações, visto que envolve todos os recursos de tecnologia de informações utilizados no ambiente. Esses recursos são fabricados por diversos fornecedores com propósitos diferentes e o técnico que dá suporte precisa estar atuante para acompanhar as atualizações, por conseguinte, o auditor também precisar acompanhar as tendências, aliás, espera-se que ele esteja à frente para proporcionar a seu cliente elementos de aconselhamento para melhoria de seus negócios.

Para Imoniana (2011), se a empresa tem um sistema de banco de dados, utiliza redes de comunicação ou tem uma configuração de *software* de sistema operacional complexa, pode ser importante que o auditor revise os controles sobre essas funções. Entretanto, para que o auditor faça sua avaliação sob o enfoque de confiabilidade dos sistemas que opera nesses ambientes, a aplicação tem que ser abrangente e ter reflexos nas operações econômicas e financeiras. Os controles e os procedimentos de controles encontrados, em geral, nesses ambientes, são frequentemente muito técnicos por natureza e podem requerer o envolvimento de especialista altamente técnico, também em auditoria de sistemas. Por isso os custos de avaliação destes controles podem ser altos. No entanto, é recomendado selecionar entre vários recursos e avaliar seus controles com base rotativa. Ou seja, revisar o sistema operacional num período, noutro período os bancos de dados, e assim sucessivamente.

Se as funções de banco de dados, sistema operacional e comunicação de dados não são adequadamente controladas, dados e programas podem ser perdidos ou alterados, controles de segurança lógica podem ser ignorados, falhas de sistema podem ocorrer mais frequentemente e, em geral, os sistemas podem não processar de forma confiável as transações econômicas e financeiras. Para Imoniana (2011, p. 135), "em ambientes de processamento menores, muitas dessas funções são feitas por fornecedores e as mudanças nesses sistemas são mínimas. Em ambientes grandes, muito complexos, o controle sobre essas funções pode se tornar muito importante".

8 PROCEDIMENTOS DE AUDITORIA DE SISTEMAS APLICATIVOS

Os procedimentos de auditoria de sistemas aplicativos referem-se àqueles executados para averiguar se os sistemas que constituem o cerne de negócio de uma empresa registram as transações rotineiras adequadamente. É uma abordagem baseada na avaliação dos sistemas das transações rotineiras para obtenção de evidências significativas da operação de tais sistemas. Essa auditoria pode ser feita quando da aquisição de um aplicativo ou quando do seu desenvolvimento interno, caracterizando uma revisão de pré-implementação. É feita também depois que o sistema é colocado em operação, entendida como pós-implantação. A efetividade dos controles internos esperados nos ambientes de sistemas aplicativos, normalmente depende dos controles de acessos a informações, controles de *hardwares*, controles organizacionais da área de processamento de dados, suporte técnico e os controles de aquisição, desenvolvimento, manutenção e documentação de sistemas refletem nos aplicativos (IMONIANA, 2011).

Conforme os sete critérios do modelo COBIT de informações, os objetivos de auditoria de sistemas, no qual aplicativos devem ser elaborados atentando para: efetividade, eficiência, confiabilidade, integridade, disponibilidade, *compliance* e confiança. Essa prescrição do modelo COBIT é válida e é bastante aplicada pelos

profissionais de auditoria de sistemas. Imoniana (2011) afirma que vale ressaltar que quando o auditor tenha ajudado na concepção e implementação dos sistemas isto o incapacita a auditar tais procedimento de controles.

8.1 COMPREENSÃO DO FLUXO DE SISTEMAS APLICATIVOS

Consiste na avaliação do uso de computadores para definir se sua aplicação é baixa, significativa ou alta no processamento dos sistemas aplicativos. Durante a auditoria, as documentações das informações referentes às estruturas dos sistemas aplicativos devem contemplar, entre outros, os seguintes pontos:

a) Identificação de sistemas-chaves:
- A identificação de sistemas-chaves é fundamental para que o auditor possa direcionar seus esforços de avaliação aos sistemas mais importantes para a consecução dos objetivos dos negócios, os quais, quando propensos a erros, poderiam apresentar variações materiais nas demonstrações financeiras. Geralmente, apresentam os fluxos de informações mais significativas.

b) Descrição do sistema:
- Levanta-se a finalidade do sistema na condução do negócio. São controles que atenuam os riscos, sejam eles controles manuais ou controles programados.

c) Descrição do perfil do sistema:
- Cita-se o volume aproximado de transações processadas por mês. Menciona os *softwares* em uso. Especifica também se o sistema foi desenvolvido internamente ou externamente, qual a linguagem de programação e quantos programas contêm.

d) Documentação da visão geral do processamento:
- *Workflow* das funções-chaves no processamento das informações significativas e a frequência de seu uso. Deve-se observar a necessidade de documentar o fluxo das transações através de Diagrama de Fluxo de Dados, enfatizando entradas-chave, lógica dos processamentos e saídas-chaves.

e) Descrição de riscos dos sistemas aplicativos:
- Deve-se documentar se o sistema opera em ambiente de produção ou de desenvolvimento; em ambas as situações, quem é o responsável? Verifique se existem versões da aplicação em uso. Se houver, quantas versões são e verifique se há planos para a eliminação de versões indesejáveis. Verifique também se há processos testados para contingências e desastres.

FONTE: Imoniana (2011, p. 140)

8.2 OBJETIVOS DE AUDITORIA

De acordo com Imoniana (2011), a auditoria de sistemas aplicativos não só tem objetivos de identificar os controles e avaliar os riscos de confidencialidade, privacidade, acuidade, disponibilidade, auditabilidade e manutenibilidade dos sistemas, mas também de concluir a respeito dos sistemas aplicativos classificados como chaves e das funções-chaves dos sistemas à consecução das missões empresariais. Os objetivos devem ser definidos em formas globais e específicas.

Segundo Imoniana (2011, p. 142), os objetivos globais referentes à auditoria de sistemas aplicativos são:

- Integridade.
- Confidencialidade.
- Privacidade.
- Acuidade.
- Disponibilidade.
- Auditabilidade.
- Versatibilidade.
- Manutenibilidade.

Já em forma específica, a auditoria de sistema aplicativo tem por objetivo certificar-se de que:

- As transações registradas nos sistemas são provenientes das operações normais da empresa.
- As transações estejam corretamente contabilizadas nos sistemas, de conformidade com os princípios fundamentais emanados das legislações vigentes.
- Os princípios sejam uniformemente aplicados nos sistemas, subsistemas e sistemas consolidadores das contas ou grupos de contas contábeis, e ainda em relação aos exercícios anteriores.
- Os controles independentes embutidos nos sistemas aplicativos sejam plenamente aplicados para certificar as consistências dos lançamentos, garantia dos processamentos e emissão dos relatórios que reflitam o resultado das transações.
- O sistema aplicativo tenha possibilidade de integrar-se inteiramente com a contabilidade geral. Ou seja, não há como se fechar as transações econômicas, financeiras e contábeis de um mês sem processar um módulo importante de sistema-chave para a geração das demonstrações financeiras.

FONTE: Imoniana (2011, p. 143)

8.3 PROCEDIMENTOS DE CONTROLES INTERNOS

A documentação dos procedimentos de controle dos sistemas aplicativos que se deseja revisar é fundamental para facilitar o apontamento dos pontos de controles que devem ser testados (IMONIANA, 2011).

Para tanto, a compreensão do fluxo de sistemas aplicativos citados anteriormente é importante. Quando da documentação desse fluxo, alguns pontos de uma forma ou de outra devem ser evidenciados. Como ênfase, Imoniana (2011, p. 143) menciona os seguintes pontos:

> a) Atribuição de responsabilidades e autoridades com perfis de acessos às pessoas e aos sistemas.
> b) Segregação das funções incompatíveis.
> c) Registro das transações de forma dependente com suas consistências de forma íntegra.
> d) Contabilização em tempo hábil.
> e) Monitoramento das operações.
> f) Levantamento de relatórios.

9 AUDITORIA DE PLANOS DE SEGURANÇA

Primeiramente, plano de segurança ou de contingência, para Imoniana (2011) significa 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 fiquem parados acarrete perdas materiais aos negócios da empresa.

O plano de continuidade, como é conhecido, numa visão secundária é muito mais que somente recuperação das atividades de informática. Segundo Imoniana (2011, p. 167), "contempla também as preocupações concernentes à vida dos funcionários, impactos sobre meio ambiente, imagens junto aos clientes e fornecedores e o público geral".

A responsabilidade básica é da diretoria da área de TI, se o ambiente for muito complexo. De acordo com Imoniana (2011), se o ambiente for moderado, é do gerente de TI, e se for ambiente pequeno, é do encarregado ou dos analistas responsáveis pela administração da rede. No entanto, para que sejam efetivas, a alta direção precisa oferecer apoio às medidas, visto que têm intuito estratégico.

Ao implementá-lo efetivamente, deve-se estabelecer os responsáveis pela consecução das ações de contingência, normalmente, as pessoas designadas a assumir ações de contingências no momento de desastres são pessoas diferentes daquelas que executam funções operacionais no dia a dia em um ambiente de TI. Segundo Imoniana (2011, p. 167), "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 transformações dos mesmos sem causar descontinuidade operacional da empresa, em caso da quebra de equipamentos ou ocorrência de algum sinistro (IMONIANA, 2011).

Para Imoniana (2011, p. 168), "no processo de implementação do plano de contingência, é recomendado que o usuário avalie-se 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: alto risco, risco intermediário e baixo risco".

Ainda de acordo com Imoniana (2011, p. 168), "após esta avaliação, o usuário deve verificar que tipo de proteção é a mais recomendada para cada caso".

9.1 OBJETIVOS DE AUDITORIA

Os objetivos da avaliação dos planos de contingências de uma empresa, segundo Imoniana (2011, p. 168), são certificar-se de que:

- Há planos desenvolvidos que contemplem todas as necessidades de contingências.
- Esses planos são suficientemente abrangentes para cobrir aspectos físicos, lógicos, de redes, de propriedades intelectuais, de pessoas, entre outros.
- A equipe de contingência está preparada para as eventualidades.
- Esses planos são testados periodicamente.
- Os *backups* podem ser recuperados com pouca ou nenhuma dificuldade.
- Há relatórios gerenciais que facilitam o acompanhamento dos procedimentos.
- Os relatórios são confiáveis.

10 AUDITORIA DE REDES

A rede empresarial é onde habita a informação que alimenta as transações e os processos de negócios. É, de acordo com Imoniana (2011, p. 177), "o local em que existem as informações mais importantes para a execução de transações não só econômicas, mas também financeiras".

A gestão efetiva desta rede concentra-se nos controles relacionados com comunicação de dados e informações nas camadas físicas e de enlace utilizando-se dos protocolos de camada de rede IP e OSI, de camadas de transporte TCP e UDP e dos protocolos de aplicação DNS, SNMP, HTTP, entre outros, para que seja confirmado o objetivo da rede na consecução das metas empresariais (IMONIANA, 2011).

"A avaliação, portanto, do processo de concepção da rede e de suas operações visa testar se suas atividades estão proporcionando aos usuários os serviços esperados". (IMONIANA, 2011, p. 177).

Outros contextos da implementação da rede e de sua operação avaliados no processo de auditoria, de acordo com Imoniana (2011, p. 177) incluem:

- Planejamento da concepção da rede com visão estratégica ao integrar o plano diretor da empresa.
- Desenho das arquiteturas e da topologia da rede.
- Implementação dos projetos físicos e lógicos.
- Monitoramento dos desempenhos e possíveis interceptações nas redes.
- Replanejamento de capacidade.
- Levantamento dos problemas operacionais e sua resolução.

Imoniana (2011) diz que vale ressaltar que as questões fundamentais relacionadas com segurança, ou seja, vulnerabilidade do TCP/IP e aplicações, deficiências, ataques às rotas, ICMP, UDP, sequência, TCP, DNS, fragmentação ou saturação de portas ou *buffer/stack overflow*, entre outras, são fundamentalmente consideradas para assegurar a confiança dos auditores com relação aos controles internos.

10.1 OBJETIVOS DE AUDITORIA

O principal objetivo de auditoria de redes, segundo Imoniana (2011, p. 178) é certificar-se da confiabilidade da rede em relação à:

- Segurança física: que contemple os equipamentos e periféricos, arquitetura da rede, sua construção e distribuição.
- Segurança lógica: que contemple as customizações dos recursos de *softwares*, em geral os rendimentos da rede, seu acompanhamento e avaliação de desempenho operacional.
- Segurança de enlace: que assegure as linhas e canais de transmissões entre unidades e localidades remotas obedecendo aos limites estabelecidos.
- Segurança de aplicação: disponibilidade da rede – poder confiar e contar com os recursos da rede quando o usuário mais precisa dela.

11 RELATÓRIOS DE AUDITORIA

Vários relatórios são emitidos em decorrência dos trabalhos de auditoria de sistemas de informações. Esses relatórios podem ser classificados em dois grupos, os que são direcionados para a consecução dos objetivos de auditoria independente e outros para atender às necessidades de auditoria interna (IMONIANA, 2011).

Quando for para atender à auditoria independente, os responsáveis pela definição dos escopos de auditoria financeira precisam dos relatórios de auditoria de sistemas enfocando aspectos de controles internos para ajudar no processo de determinação da extensão de testes substantivos e analíticos substantivos (IMONIANA, 2011).

Vale ressaltar que somente quando a estratégia de confiança nos controles for adotada e os controles que mitigam os riscos que podem existir forem identificados se recomenda avaliação dos controles internos; se não houver estabelecimento de nível aceitável e de confiança nos controles internos não se recomenda sua avaliação, pois não adianta avaliá-los, visto que a revisão apenas visa confirmar se os controles funcionam e se são efetivos. Por sua vez, quando for atender às necessidades de auditoria interna, seus relatórios ajudarão na compreensão da extensão da efetividade dos controles implementados no processo de gestão empresarial (IMONIANA, 2011).

Segundo Imoniana (2011, p. 189), os relatórios de auditoria de sistemas, em razão das facilidades do uso de informática, podem ser gerados em vários momentos das fases de auditoria:

- Após uma execução do procedimento de auditoria e constatação de fatos relevantes que podem gerar prejuízos materiais e precisam de atenção imediata e de medidas de correção urgentes.
- Relatórios interinos do processo de auditoria que visam reportar gradativamente o processo da evolução dos trabalhos e situação dos achados. Isso é fundamental no processo de auditoria interna que tem enfoque construtivo e colaborativo para aprimorar o processo de gestão.
- Relatórios preliminares emitidos após a conclusão dos trabalhos de auditoria, porém antes que o auditor saia totalmente do campo.
- Relatórios finais ou pareceres que são o produto final do trabalho de auditoria de sistemas.

De acordo com Imoniana (2011, p. 190), "os relatórios podem ser emitidos em forma final seguindo orientações de cada empresa ou até padrões de empresas auditadas. Há empresas multinacionais que possuem políticas de auditoria que definem formatos especiais de emissão desses relatórios; nesses casos, o auditor de sistemas deverá solicitar o formato para emitir o relatório".

Segundo Imoniana (2011), geralmente os relatórios finais seguem os seguintes formatos padrões e apresentam os seguintes itens: Observação – constatação do processo de auditoria; Consequências – risco em que a empresa incorre em decorrência das fraquezas apontadas; Recomendações – sugestões e medidas de correção; Comentários da gerência – concordância ou não com o ponto levantado e apontamento de prazo para implementação das medidas.

"Quando os relatórios são entregues para os responsáveis pela auditoria das demonstrações financeiras, ainda é necessário um memorando de encaminhamento apresentando os sumários dos trabalhos efetuados e as principais conclusões". (IMONIANA, 2011, p. 190).

RESUMO DO TÓPICO 2

Caro(a) acadêmico(a)! Neste tópico, você estudou que:

- A efetividade dos controles organizacionais e operacionais depende da experiência organizacional dos gestores, uma vez que exige demonstração de práticas e habilidades gerenciais.

- As funções de aquisição, desenvolvimento, manutenção e documentação de sistemas são atribuídas aos indivíduos que têm competências para conceber e implantar sistemas.

- O desenvolvimento efetivo de um sistema requer participação da alta cúpula da administração.

- O controle de *hardware* objetiva implantar procedimentos de segurança física sobre os equipamentos instalados em ambiente de informática de uma organização.

- Para que os controles de *hardware* sejam efetivos é necessário fazer inventários de *hardwares*.

- Segurança de acesso lógico refere-se à proteção dada aos recursos tecnológicos de um ambiente de sistema computadorizado contra acessos não autorizados aos dados ou informações, não permitidas a qualquer usuário, com exceção do seu proprietário. É a concessão de privilégios de acesso somente a quem tem direito ao acesso.

- A função de suporte destina-se aos usuários de TI e aos indivíduos com responsabilidade de implantar, manipular e supervisionar os recursos da tecnologia e de fornecer apoio à sua utilização nas empresas.

- Os procedimentos de auditoria de sistemas aplicativos referem-se àqueles executados para averiguar se os sistemas que constituem o cerne de negócio de uma empresa registram as transações rotineiras adequadamente.

- O plano de continuidade é muito mais que somente recuperação das atividades de informática. Ele contempla também as preocupações concernentes à vida dos funcionários, impactos sobre meio ambiente, imagens junto aos clientes e fornecedores e o público geral.

AUTOATIVIDADE

1 Cite três controles de documentação utilizados na auditoria de aquisição, desenvolvimento e manutenção de sistemas.

2 Quais os itens que normalmente são apresentados nos relatórios finais de auditoria?

3 Cite algumas operações comuns na auditoria de operação do computador.

4 Cite três funções rotineiras e três funções esporádicas na auditoria de controles de suporte técnico.

5 Quais os dois aspectos que são importantes para avaliação dos controles de acesso?

Assista ao vídeo de resolução da questão 2

NORMAS E PADRÕES DE SEGURANÇA

1 INTRODUÇÃO

Normas e padrões técnicos representam uma referência importante para a qualidade de qualquer processo. Quando processos de produção de bens e serviços são desenvolvidos em conformidade com um padrão de referência de qualidade, aumentam as garantias de que estes sejam eficientes, eficazes e confiáveis (BEAL, 2008).

"Existem diversas referências internacionais criadas para auxiliar as organizações a implementar as melhores práticas na gestão da segurança da informação e da TI". (BEAL, 2008, p. 31).

2 BENEFÍCIOS TRAZIDOS PELA ADOÇÃO DE UM PADRÃO

"Normas e padrões têm por objetivo definir regras, princípios e critérios, registrar as melhores práticas e prover uniformidade e qualidade a processos, produtos ou serviços, tendo em vista sua eficiência e eficácia". (BEAL, 2008, p. 36).

Em alguns casos, a certificação com relação à BS 17799:2 pode ser necessária para confirmar a qualidade do sistema de gestão da segurança da informação para parceiros, clientes ou fornecedores, mas para a maioria das organizações, mais importante do que buscar conformidade total ou certificação em relação a uma norma é procurar conhecer os padrões e melhores práticas disponíveis para deles extrair aquilo que puder ser útil para aprimorar seu sistema de gestão da segurança (BEAL, 2008).

Os fatores a serem considerados na adoção de um ou mais padrões de segurança incluem os objetivos de negócio, como, melhorar as operações, uniformizar processos, reduzir os riscos e que representam os recursos necessários para atingir a conformidade total ou parcial e também as vantagens de se buscar

uma certificação. Na falta de um "padrão mundial de segurança", a ISO 17799, que não oferece certificação, é útil para fornecer as diretrizes para a criação de um sistema formal de segurança da informação nas organizações (BEAL, 2008).

3 ISO GUIDE 73

A ISO/IEC Guide 73 (*Risk Management – vocabulary – guidelines for use in standards*), publicada em 2002, define 29 termos da Gestão de Riscos, os quais foram agrupados nas seguintes categorias: termos básicos; termos relacionados a pessoas ou organizações afetadas por riscos; termos relacionados à avaliação de riscos; termos relacionados a tratamento e controle dos riscos. A norma é útil para uniformizar o entendimento em relação aos conceitos relacionados ao risco (BEAL, 2008).

4 ITIL

A IT *Infrastructure Library* (ITIL) foi inicialmente publicada em 1989 pela *Central Computer Telecommunication Agency* (CCTA) (atualmente denominada de *Office of Government Commerce* (OGC)), agência do Reino Unido. Desde sua publicação original, a ITIL se propõe a ser uma fonte de boas práticas de gerenciamento de ambientes de TI, baseada na experiência de centenas de empresas de classe mundial e organizadas por um grupo de renomados especialistas em computação e administração (FOINA, 2009).

O *Information Technology Infrastructure Library* (ITIL) é uma estrutura fornecida pelo governo do Reino Unido com oito conjuntos de procedimentos de gestão: (1) prestação de serviços, (2) suporte técnico, (3) gerenciamento de serviços, (4) gestão de infraestrutura de Tecnologia de Informação e Comunicação (TIC), (5) gestão de ativos de *software*, (6) perspectiva de negócio, (7) gestão de segurança e (8) de gerenciamento de aplicações. O ITIL é uma boa opção para organizações preocupadas com suas operações (BALTZAN; PHILLIPS, 2012).

O ITIL é um conjunto de documentos desenvolvidos pelo governo do Reino Unido para registrar as melhores práticas na área de gestão de serviços de TI. Embora não represente exatamente um padrão de segurança da informação, o ITIL contempla as áreas de gestão de incidentes, problemas, configuração, atendimento ao usuário final, nível de serviço e desenvolvimento, implantação e suporte de *software*, colaborando assim tanto para a padronização e a melhoria da qualidade do serviço ofertado pela área de TI, quanto para o estabelecimento de processos voltados para o alcance dos objetivos de segurança da informação (BEAL, 2008).

A filosofia ITIL adota uma estratégia orientada a processos para atender a qualquer tipo de organização. Ela considera o Gerenciamento de Serviços em TI como um conjunto de processos estreitamente relacionados e altamente integrados.

Para atingir os objetivos-chaves do Gerenciamento de Serviços em TI, devem ser utilizadas: as pessoas, processos e tecnologias (FERREIRA; ARAÚJO, 2008).

"Dessa forma, as organizações poderão estar seguras da entrega de serviços de TI inovadores e de alta qualidade, alinhados com os processos de negócio". (FERREIRA; ARAÚJO, 2008, p. 65).

Desde o início, a ITIL foi disponibilizada sem restrições, ou seja, qualquer organização pôde utilizar a estrutura descrita nos livros. Por esse motivo, a ITIL tem sido utilizada por uma grande quantidade de organizações, como os órgãos públicos e entidades privadas (manufatura, instituições financeiras e etc.) (FERREIRA; ARAÚJO, 2008). "Os processos da ITIL podem ser utilizados como base para alcançar conformidade com as normas BS 15000 (*British Standard for IT Service Management*) e ISO/IEC 20000". (FERREIRA; ARAÚJO, 2008, p. 66).

5 COBIT

Segundo Beal (2008, p. 32),

> o COBIT é um conjunto de diretrizes para a gestão e auditoria de processos, práticas e controles de TI. Desenvolvido pela *Information Systems Audit and Control Association* (ISACA) e pelo IT *Government Institute*, o COBIT oferece um modelo de maturidade para o controle dos processos de TI e abrange práticas em quatro domínios: planejamento e organização, aquisição e implementação, entrega e suporte e monitoração.

"É um conjunto de orientações e ferramentas de apoio para a governança de TI que é aceito em todo o mundo e é geralmente utilizado por auditores e empresas como uma forma de integrar a tecnologia para aplicação de controles e cumprimento de objetivos de negócio específicos". (BALTZAN; PHILLIPS, 2012, p. 305).

"O COBIT contém mais de 300 pontos de controle para 34 processos, sendo um deles o de segurança da informação. Seu principal objetivo é auxiliar a organização a equilibrar risco e retorno de investimentos de TI". (BEAL, 2008, p. 32).

Sua estrutura de controles possui padrões aceitos mundialmente como os melhores praticados para o estabelecimento de controles e padrões de segurança para a área de Tecnologia da Informação das empresas dos mais variados segmentos de negócio. O COBIT, segundo o *site* da ISACA, foi adotado pelo *Federal Reserve* (EUA) como fonte de referência para a revisão dos sistemas de informação do sistema bancário norte-americano, demonstrando claramente sua abrangência (FERREIRA; ARAÚJO, 2008).

O CobiT está dividido em quatro domínios, dos quais 34 processos estabelecem os objetivos de controle necessários para a manutenção de uma estrutura de controles internos que possibilitem à organização atingir seus objetivos de negócio de maneira confiável (do ponto de vista de TI). Os quatro domínios são:

- Planejamento e Organização (*Plan and Organise*): abrange as estratégias e táticas, preocupando-se com a identificação da maneira pela qual a TI pode contribuir para atingir os objetivos do negócio.
- Aquisição e Implementação (*Acquire and Implement*): mudanças em um sistema aplicativo existente são cobertas por este domínio para garantir que a solução continue a atender os objetivos de negócio.
- Entrega e Suporte (*Delivery and Support*): este domínio se preocupa com a entrega dos serviços solicitados, incluindo o *Service Delivery*, a gestão da segurança da informação e continuidade, o suporte aos usuários, e o gerenciamento dos dados e das instalações.
- Monitoração e Avaliação (*Monitor and Evaluate*): os processos de TI precisam ser auditados regularmente, em sua qualidade e adequação, com os requerimentos de controle. Este domínio abrange a gestão de performance, monitoração de controles internos, conformidade regulatória.

FONTE: Ferreira e Araújo (2008, p. 58)

6 BS7799 E ISO/IEC 17799

O BS 7799 é um padrão reconhecido internacionalmente para implementação de controles de segurança.

A "família" de padrões BS 7799 trata da gestão da segurança da informação. A parte 1 desse conjunto de padrões, que corresponde a um "código de práticas para a gestão da segurança da informação", foi inicialmente publicada em 1995 pelo *British Standards Institution* (BSI) e tornou-se um padrão internacional em 2000, com sua adoção pela International Organization for Standardization (ISO) sob o nome ISO/IEC 17799 (BEAL, 2008).

O BS 7799 foi atualizado em 1999, com o objetivo de incorporar práticas de segurança em comércio eletrônico. A política de segurança pode ser definida com

base nessa referência, levando-se em consideração os pontos específicos relevantes para o contexto e a realidade de cada organização (NAKAMURA; GEUS, 2007).

De acordo com Nakamura e Geus (2007, p. 191), o padrão da *British Standard* foi desenvolvido por um comitê composto por órgãos governamentais e empresas privadas, como HSBC, Lloyds, KPGM, Shell e Unilever, e é dividido em duas partes:

- BS 7799 Parte 1, de 1995: conjunto de práticas para o gerenciamento da segurança da informação.
- BS7799 Parte 2, de 1998: especificação para sistemas de gestão de segurança da informação.

No Brasil, a ISO/IEC 17799 é publicada pela ABNT – Associação Brasileira de Normas Técnicas – sob a denominação NBR ISO/IEC 17799.

A segunda parte do padrão, BS 7799-2, é voltada para a definição de um sistema de gestão de segurança da informação (ISMS, de *Information Security Management System*). A BS 7799-2 especifica uma série de processos voltados para garantir não só a avaliação e o tratamento dos riscos, mas também a revisão e melhoria dos processos para garantir que o ISMS seja atualizado frente às mudanças no ambiente de negócios e seus efeitos na organização, e oferece certificação (BEAL, 2008).

ISMS é o acrônimo de *Information Security Management System*, o qual, traduzido para o português, quer dizer Sistema de Gestão em Segurança da Informação.

Segundo Beal (2008, p. 33),

> a certificação da parte 2 envolve uma auditoria do ISMS para verificar se a organização dispõe de processos adequados para gerenciar riscos, manter o sistema atualizado e garantir o desenvolvimento da segurança da informação. O sistema de controle implementado para gerenciar riscos deriva dos controles mencionados na ISO/IEC 17799 (o "código de prática"). O modelo de certificação e auditoria utilizado para a

> parte 2 equivale aos das normas ISO 9001 e ISO 14000, e exemplos de entidades certificadoras para a BS 7799-2 são BSI, *Certification Europe*, KEMA, KPMG e SAI *Global Limited*.

O ISO/IEC 17799 é uma versão internacional do BS 7799, adotado pela *International Standardization Organization* (ISO) e pelo *International Electricaltechnical Comission* (IEC), resultante de diversas sugestões e alterações, e existe desde 10 de dezembro de 2000. No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) traduziu a norma da ISO e conferiu-lhe a denominação de NBR ISO/IEC 17799, em 2001 (NAKAMURA; GEUS, 2007).

Assim, segundo Nakamura e Geus (2007, p. 191),

> a política de segurança pode ser definida com base em padrões de referência, como o NBR ISO/IEC 17799. Assim como as certificações em qualidade, como o ISO 9000, certificações em segurança da informação, como o ISO/IEC 17799, possuirão um valor cada vez mais crescente como diferenciais competitivos na Era da Informação. Isso demonstra a importância da política de segurança, que no Brasil é realidade em 39% das organizações. Segundo a pesquisa, 16% das organizações possuem uma política desatualizada, 30% possuem uma política em desenvolvimento e 15% não possuem uma política formalizada.

6.1 AS DEZ ÁREAS DE CONTROLE DA ISO/IEC 17799

Estas são as dez áreas de controle da ISO/IEC 17799:

- Política de segurança: recomendações para a formalização de uma política contendo diretrizes, princípios e regras que irão prover orientação e apoio para a implantação e manutenção da segurança.
- Segurança organizacional: recomendações para o estabelecimento de uma estrutura de gestão para planejar e controlar a implementação da segurança da informação na organização.
- Classificação e controle dos ativos de informação: recomendações sobre a realização de inventário dos ativos informacionais e atribuição de responsabilidades pela manutenção dos controles necessários para protegê-los.
- Segurança em pessoas: recomendações para reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações.
- Segurança física e do ambiente: recomendações para a proteção dos recursos e instalações de processamento de informações críticas ou sensíveis do negócio contra acesso não autorizado, dano ou interferência.
- Gestão das operações e comunicações: recomendações para garantir a operação correta e segura dos recursos de processamento de informações e proteger a integridade de serviços e informações.

- Controle de acesso: recomendações para o monitoramento e controle do acesso a recursos computacionais, para protegê-los contra abusos internos e ataques externos.
- Manutenção e desenvolvimento de sistemas: recomendações para o uso de controles de segurança em todas as etapas do ciclo de vida forçam que, com todos os esforços de TI, tudo seja implementado e mantido com a segurança em mente, usando controles de segurança em todas as etapas do processo.
- Gestão da continuidade do negócio: recomendações para preparar a organização para neutralizar as interrupções das atividades comerciais e proteger os processos críticos em caso de ocorrência de falha ou desastre.
- Conformidade: recomendações para a preservação da conformidade com requisitos legais (tais como direitos autorais e direito à privacidade), com as normas e diretrizes internas e com os requisitos técnicos de segurança.

FONTE: Beal (2008, p. 33)

QUADRO 17 – COMPARATIVO ENTRE ISO/IEC 17799 E BS 7799-2

ISO 17799	BS 7799-2
Visão generalista – lista de recomendações genéricas, não mensuráveis.	Especificação para um "sistema de gestão de segurança da informação" baseado nas práticas da BS 7799-1 (ISO 17799), cuja implementação é mensurável.
Não oferece certificação.	Dispõe de processo de certificação.
Usa o termo *should* (em português, traduzido por "convém que") ao descrever práticas de segurança. Exemplo: "Convém que sejam implantados controles para a detecção e prevenção de *software* malicioso, assim como procedimentos para a devida conscientização dos usuários".	Usa o termo *shall* (deve) ao descrever práticas de segurança. Exemplo: "Devem ser implementados controles de detecção e prevenção para proteção contra código malicioso e procedimentos apropriados de conscientização dos usuários".

FONTE: Adaptado de BEAL (2008, p. 35)

De acordo com Ferreira e Araújo (2008), em julho de 2007, foi alterado apenas o nome da norma NBR ISO/IEC 17799 para NBR ISO/IEC 27002.

7 ISO/IEC 13335

A ISO/IEC 13335 (*Guidelines for the management of IT security*) "é um conjunto de diretrizes de gestão de segurança voltadas especificamente para a tecnologia da informação. A norma é composta de cinco partes, que tratam de conceitos e modelos para a segurança de TI, da administração e planejamento de segurança de TI, das técnicas para a gestão da segurança de TI, da seleção de medidas de proteção e da orientação gerencial em segurança de redes. A ISO 13335 tem por objetivo não só servir de base para o desenvolvimento e o aprimoramento de uma estrutura de segurança de TI, como também estabelecer uma referência comum de gestão de segurança para todas as organizações". (BEAL, 2008, p. 35).

8 NBR ISO/IEC 27001:2006

Atualmente, existem no Brasil empresas com equipes de auditores e consultores com amplo conhecimento da norma e certificados como BS 7799 *Lead Auditor* e ISO 27001 *Lead Auditor*. Esses profissionais preparam as empresas para a certificação e acompanham o trabalho dos auditores durante o processo. Por motivos éticos, a empresa que presta consultoria no processo de preparação não efetua a auditoria de certificação (FERREIRA; ARAÚJO, 2008).

Diversas empresas no mundo já foram certificadas na norma NBR ISO/IEC 27001:2006, como bancos, empresas de telecomunicações, indústrias, prestadores de serviços, consultorias e organizações governamentais. São empresas que optaram pela certificação por vários motivos e benefícios que variam desde a redução de prêmios de seguro, até uma estratégia de *marketing* utilizando a certificação como diferencial competitivo e como demonstração pública do compromisso da empresa com a segurança das informações de seus clientes. O certificado é um atestado público de capacidade (FERREIRA; ARAÚJO, 2008).

De acordo com Ferreira e Araújo (2008, p. 56-57), o processo de certificação, resumidamente, está dividido em:

> • Revisão da documentação do ISMS de acordo com as normas NBR ISO/IEC 27001:2006 e NBR ISO/IEC 27002:2005.
> • Visita inicial para a obtenção de informações antes da auditoria, e determinação do escopo.
> • Auditoria de Certificação que consiste na realização de entrevistas e análise do ISMS em operação.
> • Emissão do Certificado, desde que o ambiente esteja em conformidade com a norma.
> • Auditoria anual, para certificar que o ISMS continua operando satisfatoriamente.

Vale ressaltar que a renovação do certificado deve ser efetuada a cada três anos e exige-se que seja realizada uma nova Auditoria de Certificação (FERREIRA; ARAÚJO, 2008). O custo da certificação depende de vários fatores, tal como quanto

tempo o responsável pela certificação levará para se convencer sobre a conformidade das instalações da organização com relação à norma, ao tamanho e à complexidade da empresa e de seus sistemas (FERREIRA; ARAÚJO, 2008).

9 SARBANES-OXLEY

O ato Sarbanes-Oxley, elaborado pelo senador americano Paul Sarbanes e pelo deputado Michael Oxley, tornou-se lei em 30 de julho de 2002 e introduziu mudanças significativas à governança corporativa e ao cenário financeiro, visando "proteger os investidores através da melhoria dos processos que geram as demonstrações financeiras". (FERREIRA; ARAÚJO, 2008, p. 143).

Foi criada para aperfeiçoar os controles internos financeiros das organizações que possuem ações na Bolsa de Nova York (*New York Stock Exchange*). Esta lei, que também atinge empresas brasileiras, veio em decorrência dos escândalos financeiros das empresas Enron, Worldcom e outras, que acabaram com as economias pessoais de muitos norte-americanos (FERREIRA; ARAÚJO, 2008).

A SOX, como é conhecida, prevê multas que variam de US$ 1 milhão a US$ 5 milhões e penas de reclusão entre 10 e 20 anos para seus executivos, CEOs (*Chief Executive Officer*), CFOs (*Chief Finance Officer*) e outros demais envolvidos (FERREIRA; ARAÚJO, 2008).

O principal objetivo da lei é estimular as organizações a buscarem mais eficiência na Governança Corporativa, o que também depende de um gerenciamento de riscos bem-sucedido. Além de garantir maior controle com as contas das organizações, a lei também contribuiu para as companhias acelerarem seus processos de gestão de riscos corporativos (FERREIRA; ARAÚJO, 2008).

A SOX está organizada em 11 partes, cada qual contendo um número de seções. As seções consideradas mais significativas da SOX com relação à conformidade e controles internos são: 302, 404 (mais visada), 401, 409, 802 e 906 (FERREIRA; ARAÚJO, 2008).

A partir dessa lei, os Executivos Financeiros têm de assinar os relatórios financeiros da empresa. Também, significa que atestam a veracidade das informações pessoalmente, ou seja, podem pagar até mesmo com o patrimônio pessoal se forem descobertas irregularidades – FRAUDES (FERREIRA; ARAÚJO, 2008).

Cada vez mais os sistemas de TI estão automatizando as atividades de negócio e fornecendo mais funcionalidades que permitem ter maior ou menor controle. Consequentemente, há necessidade de incluir controles de TI para os sistemas financeiros existentes (FERREIRA; ARAÚJO, 2008, p. 144).

Ferreira e Araújo (2008, p. 144) comentam que, resumidamente, os executivos têm os seguintes desafios:

- Aprimorar o seu conhecimento sobre controles internos.
- Entender como estar em conformidade com a SOX.
- Desenvolver um plano específico de conformidade para aprimoramento dos controles internos de TI.
- Integrar este plano à estratégia da organização.
- Entender o programa de controles internos da organização e o processo de demonstrações financeiras.
- Mapear os sistemas de TI que suportam o processo de reporte financeiro para elaboração das demonstrações e os controles internos.
- Identificar os riscos relacionados a esses sistemas.
- Desenhar e implementar controles para minimizar os riscos identificados e monitorá-los continuamente.
- Documentar e testar os controles de TI.
- Assegurar que os controles de TI estejam atualizados e sejam alterados quando necessário.

O tema segurança da informação foi amplamente beneficiado com o advento SOX, pois muitos dos requisitos de segurança, que antes não eram justificados, em virtude da lei conseguiram sua respectiva aprovação orçamentária, além da priorização de execução (FERREIRA; ARAÚJO, 2008).

LEITURA COMPLEMENTAR

Caros(as) acadêmicos(as)! Como leitura complementar, segue um texto sobre a importância de uma auditoria de sistemas independentes. Veremos como o assunto é tratado sob a ótica de Carlos Marcelo Lauretti, profissional com extensa experiência como gestor de TI em empresas de grande porte dos setores de engenharia civil e editorial.

A importância de uma auditoria de sistemas independente

A maioria das grandes empresas está obrigada a se submeter a auditorias independentes durante as quais normalmente está incluída uma auditoria de sistemas. Lamentavelmente, muitas empresas, especialmente as de pequeno e médio porte não estão obrigadas às auditorias externas, portanto, a área de informática não tem que prestar contas de seus procedimentos e ações além da própria direção.

A auditoria independente é o instrumento que as empresas têm para assegurar aos seus acionistas de que seguem as melhores práticas de governança corporativa. Sem uma auditoria independente não há como garantir a confiabilidade das informações que são disponibilizadas. Assim como não se pode confiar nos demonstrativos contábeis de uma empresa se eles não passarem por um controle independente, também não é possível confiar nos sistemas de informações destas organizações se não estiverem sujeitos a auditorias de sistemas independentes e rotineiras.

Em muitos anos à frente da TI de várias empresas, sempre me defrontava com a suspeita se as informações disponibilizadas pelos sistemas eram confiáveis. Meus problemas terminaram quando passei a ser submetido à auditoria independente. A auditoria independente assegurava à empresa, que eu adotava todas as práticas necessárias para garantir a integridade dos sistemas.

Profissionais de TI não devem ver auditorias externas como ameaças ao seu trabalho. Ao contrário, bons profissionais querem demonstrar à empresa que podem confiar em seus sistemas de informação. Em muitas situações, a auditoria externa até mesmo corrobora as solicitações de TI para implantar soluções mais robustas, como por exemplo, relativas à tolerância a falhas, segurança de acessos e outras necessidades que muitas vezes não somos capazes de convencer a alta direção de efetuar os investimentos necessários.

Para as empresas que não estão sujeitas à obrigatoriedade de uma auditoria de sistemas, é extremamente vantajoso que as façam espontaneamente. Os resultados são ainda melhores quando a iniciativa desta auditoria parte da própria área de TI. Muitos profissionais de TI equivocadamente veem a auditoria de sistemas como uma ameaça. É extremamente preocupante empresas nas quais a TI vê a auditoria como uma ameaça e não como uma aliada.

Uma experiência muito interessante é a alta direção propor à TI a utilização de uma auditoria de sistemas. Sem dúvida, naquelas que houver uma rejeição muito grande, ou disserem que é jogar dinheiro fora, deve-se iniciar imediatamente esta auditoria independente. Aquelas que tiverem o apoio de TI se pode deixar para um momento mais oportuno.

FONTE: Disponível em: <http://www.tiespecialistas.com.br/2011/02/a-importancia-de-uma-auditoria-de-sistemas-independente/>. Acesso em: 24 jul. 2013.

RESUMO DO TÓPICO 3

Caro(a) acadêmico(a)! Neste tópico, você estudou o seguinte:

- Normas e padrões técnicos representam uma referência importante para a qualidade de qualquer processo.

- Os fatores a serem considerados na adoção de um ou mais padrões de segurança incluem os objetivos de negócio, os recursos necessários para atingir conformidade total ou parcial e as vantagens de se buscar uma certificação.

- A norma ISO/IEC Guide 73 é útil para uniformizar o entendimento em relação aos conceitos relacionados ao risco.

- O ITIL é um conjunto de documentos desenvolvidos pelo governo do Reino Unido para registrar as melhores práticas na área de gestão de serviços de TI e adota uma estratégia orientada a processos para atender a qualquer tipo de organização.

- A estrutura de controles do COBIT possui padrões aceitos mundialmente como melhores práticas para estabelecer controles e padrões de segurança para a área de TI das empresas dos mais variados segmentos de negócio.

- O BS 7799 é um padrão reconhecido internacionalmente para implementação de controles de segurança.

- A ISO/IEC 17799 é uma versão internacional do BS 7799, resultante de diversas sugestões e alterações. No Brasil, a ABNT traduziu a referida norma sob a denominação de NBR ISO/IEC 17799.

- A ISO/IEC 13335 é um conjunto de diretrizes de gestão de segurança voltadas especificamente para a tecnologia da informação.

- O principal objetivo da lei Sarbanes-Oxley é garantir a fidedignidade nos resultados das companhias e também estimular as organizações a buscarem mais eficiência na Governança Corporativa.

AUTOATIVIDADE

1 Explique o que vem a ser o ITIL e qual é seu objetivo.

2 Cite os quatro domínios do COBIT.

3 O que vem a ser a norma ISO/IEC 13335?

4 Qual é a versão mais atual da norma NBR ISO/IEC 17799?

5 O que motivou a criação da Lei Sarbanes-Oxley?

Assista ao vídeo de resolução da questão 3

REFERÊNCIAS

BALTZAN, Paige; PHILLIPS, Amy; **Sistemas de informação**. Porto Alegre: AMGH, 2012.

BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

BERNSTEIN, Terry; BHIMANI, Anish B.; SCHULTZ, Eugene; SIEGEL, Carol A. **Segurança na internet**. Rio de Janeiro: Campus, 1997.

BRASIL. **Manual de auditoria de sistemas – tribunal de contas da união**. Brasília: TCU, Secretaria de Auditoria e Inspeções, 1998. Disponível em: <www.facape.br/cynara/sas/Manual_TCU_Audit_Sistemas.pdf>. Acesso em: 18 jan. 2013.

CARMONA, Tadeu. **Segurança e espionagem digital**. 2. ed. São Paulo: Digerati Books, 2007.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações**. 2. ed. rev. e ampl. São Paulo: Editora SENAC São Paulo, 1999.

COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim. **Distributed systems**: concepts and design. 3. ed. England: Addison Wesley, 2001.

COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim. **Sistemas distribuídos**: conceitos e projeto. 4. ed. Porto Alegre: Bookman, 2007.

CYCLADES Brasil. **Guia internet de conectividade**. 8. ed. São Paulo: SENAC, 2001.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação – guia prático para elaboração e implementação**. 2. ed. revisada. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

FOINA, Paulo Rogério. **Tecnologia da informação**: planejamento e ges**tão.** São Paulo: Atlas, 2009.

FONTES, Eduardo. **Segurança da informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

GIL, Antonio de Loureiro. **Auditoria de computadores**. 5. ed. São Paulo: Atlas, 2000.

GROSS, Jan Charles. **Sistemas distribuídos**. Indaial: Ed. Asselvi, 2008.

IMONIANA, Joshua Onome. **Auditoria de sistemas de informação**. 2. ed. São Paulo: Atlas, 2011.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de informações gerenciais**: administrando a empresa digital. São Paulo: Pearson Prentice Hall, 2004.

MONTEIRO, Emiliano Soares. **Segurança em ambientes corporativos**. Florianópolis: Visual Books, 2003.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

SCHMIDT, Paulo; SANTOS, José Luiz dos; ARIMA, Carlos Hideo. **Fundamentos de auditoria de sistemas**. São Paulo: Atlas, 2006.

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

STAIR, Ralph M.; REYNOLDS, George W. **Princípios de sistemas de informação**. 9. ed. São Paulo: Cengage Learning, 2011.

VERTON, Dan. **Diário hacker**: confissões de hackers adolescentes. São Paulo: Berkeley Brasil, 2002.

WEBER, Kival Chaves. ROCHA, Ana Regina Cavalcanti da; NASCIMENTO, Célia Joseli do. **Qualidade e produtividade em software**. 4. ed. renovada. São Paulo: Makron Books, 2001.