

NEWS

Felipe Veronezi
Alex Pinheiro das Graças

SEGURANÇA E AUDITORIA
DE SISTEMAS

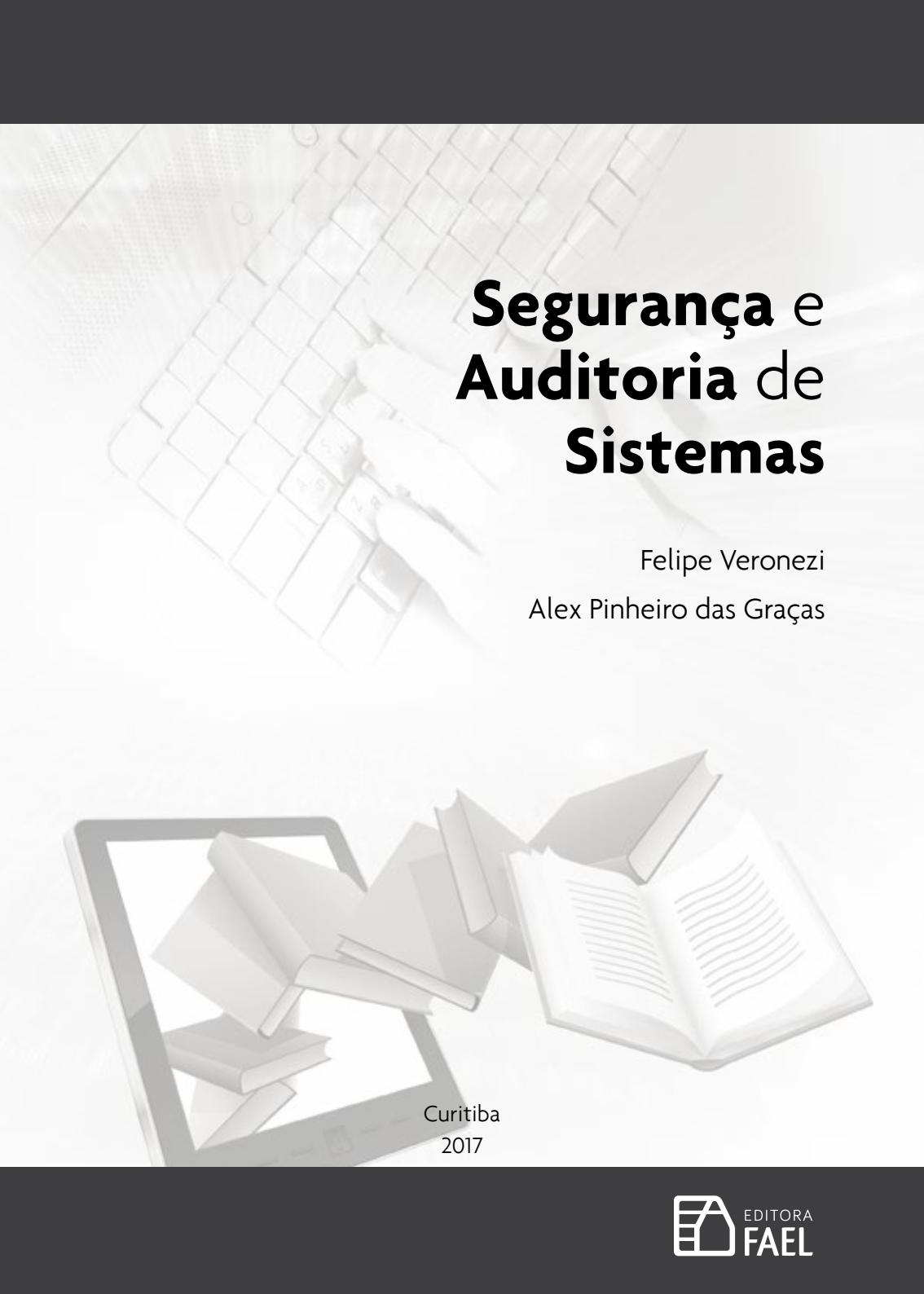
Tecnologia



SEGURANÇA E AUDITORIA DE SISTEMAS

Felipe Veronezi
Alex Pinheiro das Graças





Segurança e Auditoria de Sistemas

Felipe Veronezi
Alex Pinheiro das Graças



Curitiba
2017

Ficha Catalográfica elaborada pela Fael. Bibliotecária – Cassiana Souza CRB9/1501

V549s Veronezi, Felipe

Segurança e auditoria de sistemas / Felipe Veronezi, Alex Pinheiro das Graças. – Curitiba: Fael, 2017.

304 p.: il.

ISBN 978-85-60531-78-3

1. Computadores – Medidas de segurança 2. Sistemas de telecomunicações – Medidas de segurança I. Graças, Alex Pinheiro das II. Título

CDD 005.8

Direitos desta edição reservados à Fael.

É proibida a reprodução total ou parcial desta obra sem autorização expressa da Fael.

FAEL

Direção Acadêmica Francisco Carlos Sardo

Coordenação Editorial Raquel Andrade Lorenz

Revisão Editora Coletânea

Projeto Gráfico Sandro Niemicz

Capa Vitor Bernardo Backes Lopes

Imagen da Capa Shutterstock.com/Arcady/Sergey Nivens

Arte-Final Evelyn Caroline dos Santos Betim

Sumário

CARTA AO ALUNO | 5

1. CONCEITOS E Princípios de Segurança da Informação | 7
2. METODOLOGIAS e Padrões de Segurança da Informação | 35
3. PROCEDIMENTOS e Boas Práticas de Segurança da Informação | 65
4. ASPECTOS TECNOLÓGICOS da Segurança da Informação | 103
5. ASPECTOS HUMANOS da Segurança da Informação | 139
6. GERENCIAMENTO DE Riscos em Segurança da Informação | 159
7. FUNDAMENTOS EM Auditoria de Sistemas de Informação | 183
8. METODOLOGIA DE Auditoria de Sistemas de Informação | 209
9. TÉCNICAS e Melhores Práticas de Auditoria de Sistemas de Informação | 233
10. FERRAMENTAS DE Auditoria de Sistemas de Informação | 263

CONCLUSÃO | 283

GABARITO | 285

REFERÊNCIAS | 299

Carta ao Aluno

PREZADO(A) ALUNO(A),

A ÁREA DE SEGURANÇA da informação está cada vez mais em evidência. A popularização do acesso à internet trouxe inúmeros benefícios, porém também trouxe muitas preocupações, em especial com aqueles que não possuem conhecimento de informática suficiente para prevenir-se de armadilhas nos ambientes computacionais.

Segurança e Auditoria de Sistemas

Com o domínio desta área de conhecimento, você será capaz de auxiliar gestores de organizações a proteger um de seus bens mais valiosos: a informação! Perceberá também que muitas coisas podem ser aplicadas em sua vida pessoal, como o cuidado que se deve ter com suas senhas e arquivos pessoais.

Finalmente, o estudo de auditoria de sistemas o auxiliará a ser um profissional zeloso quanto à identificação de falhas e irregularidades nos sistemas de informação, bem como nos processos de uma organização.

Bons estudos!

1

Conceitos e Princípios de Segurança da Informação

VIVEMOS A ÉPOCA denominada “era da informação”. A produção de informações cresce de maneira exponencial, de modo que as novas gerações possuem muito mais acesso às informações e de maneira muito mais ágil do que as gerações anteriores. Da mesma forma que cresce a produção e acesso às informações, deve crescer também o cuidado com a gestão segura destas informações por parte das organizações. O relatório do CERT.BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) aponta que no ano de 2015 ocorreram mais de 720 mil incidentes de segurança reportados (CERT.br, 2016). Alguns destes incidentes representaram perdas significativas em termos de ativos financeiros para as organizações.

NESTE CAPÍTULO ABORDAREMOS conceitos fundamentais de segurança da informação, como seus pilares básicos e suas formas de classificação. Apresentaremos também o ciclo de vida de uma informação dentro de um ambiente corporativo, bem como quais

são os passos básicos para a implantação de uma política de segurança da informação eficiente.

Ao final deste capítulo você será capaz de compreender que um dos ativos mais importantes de uma empresa ou organização é a informação. Também compreenderá que a gestão de forma segura desta massa de dados poderá ser um diferencial a nível pessoal e corporativo, pois tal gestão afeta diretamente todos os negócios de uma empresa ou indivíduo.

Objetivo de aprendizagem:

- × Compreender a importância de proteger a informação, bem como ser capaz de gerenciá-la dentro de padrões reconhecidos no ambiente corporativo.

1.1 Dados, informação e conhecimento

Antes de avançarmos no estudo da segurança da informação é importante compreendermos a diferença dos conceitos de dados, informação e conhecimento. Você irá perceber que são conceitos complementares e ligados diretamente um ao outro. Ao perceber a diferença e relação entre os conceitos, ficará mais claro o motivo pelo qual as informações necessitam ser protegidas nos ambientes corporativos. Em alguns casos, para pessoas e empresas, a informação chega a ser o seu ativo mais valioso!

× **Dados**

São os elementos fundamentais e brutos, ou seja, a matéria-prima da informação. Se você possui apenas dados brutos, não será possível tomar uma decisão somente baseada nestes dados. Eles são fundamentais em uma organização, desde que sejam trabalhados a fim de gerar informação e conhecimento.

× **Informação**

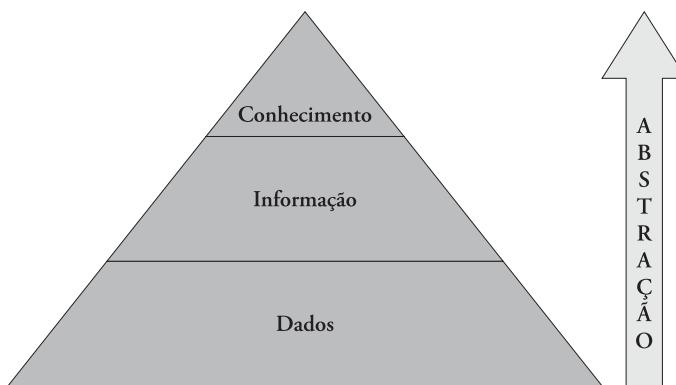
É o conjunto de dados organizado de forma ordenada a fim de transmitir um significado dentro de um contexto. A informação nos dá a capacidade de tomar decisões sobre os mesmos dados que, isoladamente, não faziam muito sentido para nós.

✗ **Conhecimento**

É o maior nível de abstração, quando um conjunto de informações constitui um saber sobre determinado assunto. A informação passa a ter um valor agregado e podemos utilizá-la para um determinado propósito.

Agora podemos perceber que quanto mais nos distanciarmos dos dados brutos, maior é o nível de abstração que iremos alcançar, ou seja, aumentamos a capacidade de subtrair detalhes, de modo que possamos visualizar algo de forma mais concisa. Vide figura 1.1 a seguir.

Figura 1.1 – Nível de abstração



Fonte: Elaborada pelo autor.

Vamos tentar compreender melhor estes conceitos por meio de um exemplo prático. Observe as palavras a seguir.

VERDE | GRANDE | CASA

Isoladamente, estas palavras não nos trazem muito significado. Por exemplo, se dissermos a palavra “grande”, não podemos chegar a alguma conclusão. O que é grande? Ou então, analisando a palavra “verde”, isoladamente, sabemos que refere-se a uma cor, mas isto não representa um conceito completo.

Quando organizamos os dados, no caso as palavras anteriores, podemos obter um conceito completo, que antes da organização não teríamos como

saber. Trata-se de obter uma informação por meio da organização dos dados, como por exemplo: “a casa verde é grande”.

Agora vamos adicionar mais um dado neste exemplo (mais uma palavra): “grama”. Podemos então reorganizar estes dados e obter uma informação completamente diferente da primeira: “a grama verde da casa está grande”.

Percebemos então que dados brutos podem não representar algo significativo dentro de uma organização. Já a informação gerada a partir destes dados possui valor agregado. E por possuir valor é que necessitamos pensar em formas de proteger a informação. Agora que compreendemos a diferença conceitual, temos melhores condições de compreender também como a informação torna-se um ativo tão valioso dentro de uma organização.

1.2 Conceitos de segurança da informação

As organizações de modo geral possuem hoje uma grande quantidade de dados armazenados em forma de informação decisiva para os gestores. Estas informações podem representar informações financeiras, segredos comerciais, arquivos confidenciais, oportunidades de negócios, dentre outros diversos tipos.

Muitas informações são tão valiosas que é necessário empregar recursos com o objetivo de protegê-las. Enquanto alguns querem proteger as informações, outros querem acessá-las por qualquer meio, inclusive para fins ilícitos. Por exemplo, dados armazenados em bases do Detran de cada unidade da federação possuem endereços atualizados de diversos cidadãos. Se estas informações caírem em mãos de pessoas mal-intencionadas, isto pode representar um risco à integridade física de um proprietário de veículo.

Para que uma informação possa ser repassada entre diversos atores, é necessário um mecanismo de transmissão. Esta transmissão, também denominada comunicação, pode ser em tempo real, como em uma transmissão de vídeo ao vivo, ou então ela pode ser armazenada para posteriormente ser acessada, como por exemplo no armazenamento de dados digitais em um *data center*, ou em um armazenamento físico, como em um livro.

A comunicação é composta de alguns elementos básicos:

- ✖ **mensagem** – é o objeto da comunicação, uma ideia, conceito, ou informação propriamente dita. É composta de um código conhecido, que pode ser composto por palavras de uma determinada língua ou ainda linguagem binária de máquina, dentre outros.
- ✖ **emissor** – é quem deseja transmitir a mensagem que pode ser produzida por ele mesmo ou obtida de outras fontes.
- ✖ **canal** – é o meio pelo qual a mensagem é enviada.
- ✖ **receptor** – é o destinatário final da mensagem. Para que seja corretamente compreendida e interpretada, é necessário que o receptor possua o conhecimento do mesmo código no qual a mensagem foi composta.

A fim de se evitar problemas no processo de comunicação, bem como garantir a eficácia e segurança da informação, devem ser seguidas normas que se enquadram em conceitos conhecidos como pilares da segurança da informação.

1.2.1 Pilares de segurança da informação

A segurança da informação possui três pilares básicos que iremos detalhar a seguir.

- ✖ **Confidencialidade:** é o conceito de que determinadas informações só podem ser acessadas por quem é de direito conhecê-las, ao mesmo tempo que impede o acesso não autorizado a elas. No mundo corporativo torna-se fundamental proteger o capital intelectual agregado nas informações que a empresa ou pessoa possui. Um vazamento pode significar a perda de vantagem competitiva de mercado.
- ✖ **Integridade:** é a garantia de que a informação armazenada é verdadeira e não está corrompida. Esta informação armazenada deve conter exatidão e manter todas as propriedades originais definidas por seu proprietário.
- ✖ **Disponibilidade:** é a propriedade de que a informação deve estar disponível sempre que alguém autorizado, no exercício de suas funções, necessitar dela. Quando uma informação importante fica

indisponível em uma empresa, todos os processos que dependem dela ficam paralisados.

Você sabia

Os três pilares da segurança da informação são conhecidos no mundo corporativo como *Tríade CID*, ou simplesmente *CID*.

Além destes três aspectos principais, segundo Lyra (2008), outros conceitos complementam a segurança da informação, sendo eles:

- × **autenticação** – é a garantia de que um usuário é de fato quem alega ser, sendo que a fonte da informação deve ser assegurada.
- × **não-repúdio** – também conhecido como irretratabilidade, é a capacidade de provar que um usuário foi responsável por determinada ação. Isto vale para quem emite e quem recebe a informação.
- × **legalidade** – é a propriedade que garante que a informação está de acordo com a legislação pertinente, podendo estar relacionada com cláusulas contratuais ou legislação nacional e internacional.
- × **privacidade** – é a capacidade de um usuário efetuar determinadas ações de maneira anônima, impossibilitando o relacionamento entre este usuário e suas ações.
- × **auditoria** – fornece transparência aos negócios, pois deve garantir que tudo o que foi realizado pelos usuários possa ser auditado, detectando fraudes ou até mesmo tentativas de ataques.

Saiba mais

Dentre os conceitos complementares, a autenticação e legalidade são comumente associadas aos três pilares básicos CID, construindo a sigla CIDAL.

Apresentaremos um exemplo fictício de uma situação vivenciada em um ambiente corporativo, de modo que possamos compreender melhor como os pilares da segurança da informação fazem parte do dia-a-dia de uma organização.

Agora vamos compreender melhor estas propriedades por meio de um exemplo fictício prático:

“Maria é funcionária do RH de uma grande corporação. As informações salariais são de acesso exclusivo a funcionários do RH e diretores (**confidencialidade**). Maria deseja gerar um ambiente de discordia na empresa e envia uma planilha com salários adulterados para uma lista de e-mails internos de funcionários de outros setores. Um dos funcionários comunica sua chefia, que por sua vez comunica a direção da empresa. Eles compararam a planilha enviada por Maria, com a planilha contida em uma pasta de rede do servidor, cujo acesso é somente leitura (**integridade**). Quando chamam Maria para conversar, eles tentam acessar a mesma planilha, porém uma falha no ponto de rede impede o acesso instantâneo (**disponibilidade**). Resolvido o problema eles conversam com Maria, que admite a alteração dos valores da planilha salarial original e envio da mesma. Maria é então demitida por justa causa.”

Saiba mais

Um incidente de segurança é quando ocorre uma violação de algum dos aspectos acima listados, podendo acarretar interrupção nos processos de negócio de uma organização.



1.2.2 Conceitos complementares de segurança da informação

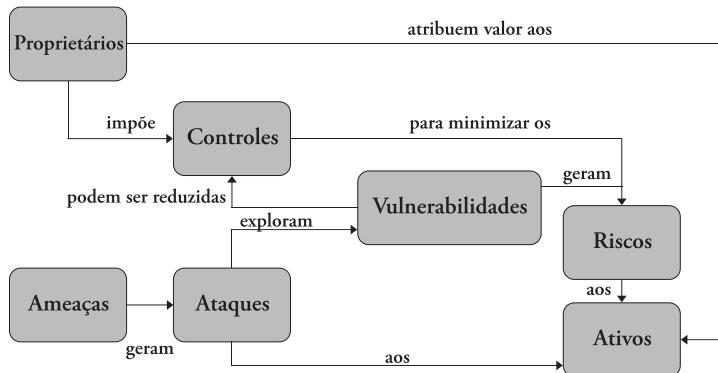
Além dos principais aspectos que sustentam a segurança da informação, é necessário compreendermos conceitos complementares, os quais seguem.

- × **Ativo de informação:** o termo “ativo” é muito utilizado nos textos de normas como a ISO/IEC 27001 (estudaremos as normas no capítulo 2). Entende-se como ativo da informação a própria informação somada a qualquer componente que a sustenta ou se utiliza dela. Este componente pode ser humano, tecnológico, hardware, software, entre outros. Detalharemos a classificação dos ativos no próximo tópico.
- × **Ataque:** é a exploração de uma falha por um agente, motivado por fatores diversos, atingindo algum ativo de valor.
- × **Vulnerabilidade:** é o ponto fraco de um ativo. A vulnerabilidade não caracteriza a quebra imediata de um dos pilares CID. A quebra ocorre quando a mesma é explorada por um agente externo.
- × **Ameaça:** é a iminência de um ataque, caracterizado pela exposição de uma vulnerabilidade a um meio hostil.
- × **Probabilidade:** é a quantificação das chances de um ataque ser efetivado contra um ativo, levando em conta as ameaças e vulnerabilidades. Observe que, se um ativo possui várias vulnerabilidades, mas as chances de ataque são próximas de zero, consequentemente a probabilidade do ativo ser comprometido será próxima de zero também.
- × **Contra-medidas:** são técnicas e métodos utilizados para a defesa contra ataques, bem como a mitigação de vulnerabilidades.
- × **Impacto:** o impacto está em uma relação de direta proporcionalidade com as consequências que um incidente de segurança pode causar. Quanto maior o valor do ativo maior também será o impacto, caso um incidente de segurança seja concretizado.
- × **Controle:** são os meios utilizados para resolução das vulnerabilidades. Este controle pode ser efetuado utilizando-se de um equipa-

mento (por exemplo, um *firewall*), ou então por meio do ajuste de um processo, ou ainda pela implantação de uma nova tecnologia.

Podemos compreender melhor o relacionamento entre estes conceitos por meio da figura a seguir.

Figura 1.2 – Relacionamento entre conceitos complementares



Fonte: Adaptado de Fagundes (2012).

Saiba mais

Relatos de incidentes de segurança são frequentemente catalogados por empresas que atuam neste ramo. Como curiosidade você pode acessar os principais incidentes ocorridos no ano de 2014 em: <<http://www.tecmundo.com.br/seguranca/73110-12-principais-incidentes-seguranca-informacao-2014.htm>>.

Você percebe o quanto um incidente de segurança pode ser prejudicial para a imagem de uma organização?

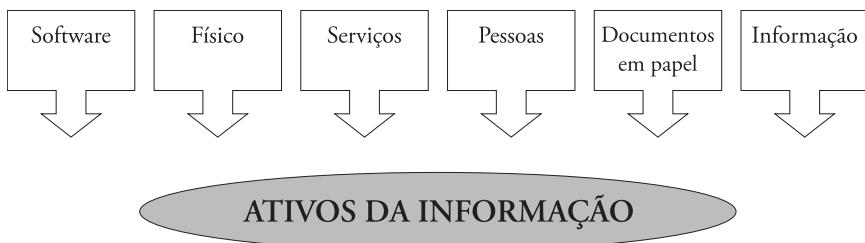
1.3 Classificação das informações

Segundo Lyra (2008, p. 13), “a classificação da informação é o processo pelo qual estabelecemos o grau de importância das informações frente a seu

impacto no negócio ou processo que elas suportam. Ou seja, quanto mais estratégica ou decisiva para o sucesso do negócio, mais importante a informação será”.

Para que possamos compreender a classificação das informações, é necessário separá-las em grupos, os ativos da informação, explanados no tópico anterior. A figura 1.3 e o quadro 1.1 demonstram melhor esta classificação:

Figura 1.3 – Ativos da informação



Fonte: Elaborada pelo autor.

Quadro 1.1 – Classificação dos ativos

Natureza do Ativo	Ativos de informação
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, nobreak e ar-condicionado
	Móveis, prédios e salas

Natureza do Ativo	Ativos de informação
Serviços	Computação (aplicação de patches, backup)
	Comunicação (ligações telefônicas, videoconferências)
	Utilidades gerais
Pessoas	Empregados, estagiários, terceiros e fornecedores
Documentos em papel	Contratos
	Documentação da empresa
	Relatórios confidenciais
Informação	Banco de dados e arquivos magnéticos
	Documentação de sistemas e manual do usuário
	Material de treinamento
	Procedimentos operacionais de recuperação
	Planos de continuidade

Fonte: Ferreira; Araújo (2008).

A classificação deve levar em conta o fato de que necessita ser de fácil compreensão e claramente descrita na política de segurança da informação, a qual iremos detalhar no próximo tópico. Também deve estar centrada nos quatro principais eixos CIDAL: confidencialidade, disponibilidade, integridade e autenticidade.

1.3.1 Classificação quanto à confidencialidade

Podemos classificar as informações em quatro níveis de acesso, sendo eles:

- ✗ **nível 1 – informação pública:** são informações que não trarão prejuízo caso sejam divulgadas fora da organização.
- ✗ **nível 2 – informação interna:** a divulgação externa deve ser evitada, embora caso aconteça, não incorre em prejuízo significativo para a organização.

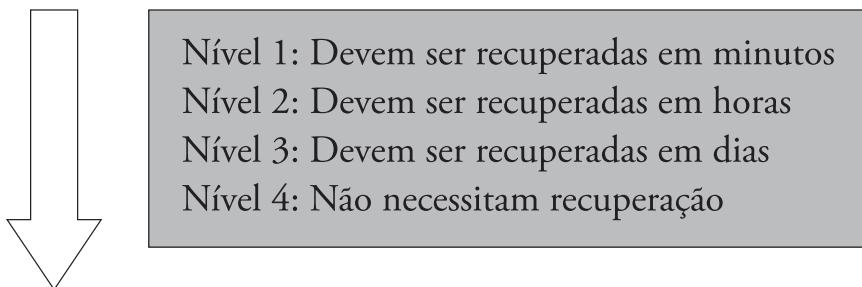
- × **nível 3 – informação confidencial:** estas informações devem ter acesso restrito ao ambiente interno da organização. Sua divulgação pode acarretar em perdas financeiras e de competitividade.
- × **nível 4 – informação secreta:** a restrição deve ser exclusivamente ao ambiente interno e de forma muito controlada, somente pessoas específicas devem ter acesso a informação. Sua divulgação trará alto impacto à organização.

1.3.2 Classificação quanto à disponibilidade

Observe a seguinte pergunta: o quanto uma informação faz falta dentro de uma instituição?

Para responder a essa pergunta iremos classificar as informações de acordo com o tempo em que elas devem ser recuperadas:

Figura 1.4 – Classificação quanto à disponibilidade



Fonte: Lyra (2008).

1.3.3 Classificação quanto à integridade

Para classificar a informação de acordo com este critério é necessário identificar aquelas que são fundamentais ao negócio, assim os esforços podem ser direcionados no sentido de prevenir, detectar e corrigir a produção de informações sem integridade.

1.3.4 Classificação quanto à autenticidade

Quando for necessário a divulgação de informações ao público externo é imprescindível que tais informações apresentem requisitos de verificação e autenticidade.

Importante

Uma vez efetuada a classificação das informações deve-se implementar procedimentos para o monitoramento contínuo pela área responsável pela segurança da informação, a fim de assegurar que, com o passar do tempo, cada ativo esteja adequadamente classificado.

1.4 Ciclo de vida da informação

De um modo geral, a expressão “ciclo de vida” refere-se a um conjunto de etapas que um determinado agente passa durante sua existência. Por exemplo, no âmbito da biologia uma borboleta começa sua vida como um ovo, que eclode e passa para um estágio de larva, que por sua vez transforma-se em pupa para finalmente, virar um animal adulto.

As informações também passam por estágios dentro de uma organização. Lyra (2008) organiza este ciclo de vida da informação em seis etapas, dispostas conforme a figura 1.5, as quais iremos detalhar a seguir:

Figura 1.5 – Ciclo de vida da informação



Fonte: Lyra (2008).

Tudo começa na etapa de **obtenção**, quando uma informação é criada, ou ainda obtida por meio de uma fonte externa.

A etapa de **tratamento**, ou manuseio, é quando a informação necessita de algum tipo de organização ou formatação para que possa se tornar acessível a outros utilizadores. Via de regra é necessário também o **armazenamento** da informação, a fim de assegurar a conservação para uso futuro.

A próxima etapa é a **distribuição**, onde deve-se fazer chegar a informação a quem necessitar dela em um determinado momento. O **uso** da informação é quando é gerado valor agregado para a organização. E finalmente na etapa de **descarte**, é realizado o expurgo de informações que não são mais úteis ou que se tornaram obsoletas.

Saiba mais

Você notou que em cada uma destas etapas, os aspectos da tríade CID (confidencialidade, integridade e disponibilidade) não só podem como devem ser aplicados? Por exemplo, ao tratar uma informação é necessário garantir que a mesma continue íntegra em todos os seus aspectos. Ou então, na etapa de armazenamento, quando uma informação é sigilosa deve ser observado a confidencialidade no controle de acesso posterior, bem como a disponibilidade de acordo com o nível de criticidade.

Importante

No processo de descarte, deve ser observado o impacto que cada informação oferece à instituição, caso haja um vazamento de informação classificada! Por exemplo, informação em papel que necessita de confidencialidade, deve ser triturada antes do descarte.

1.5 Política de segurança da informação

Toda organização necessita minimizar os riscos de segurança por meio da implementação de uma política de segurança da informação eficiente,

de acordo com seus sistemas internos, cultura e necessidades. Esta política deve ser criada, preferencialmente, antes da ocorrência de um problema de segurança. Trata-se do estabelecimento de regras e padrões para assegurar a proteção das informações, de acordo com os critérios de confidencialidade, integridade e disponibilidade (CID).

É bem comum, no ambiente corporativo, que ao iniciarmos um projeto de segurança, os atores envolvidos tenham um desconhecimento geral dos ambientes e processos da instituição. Isto ocorre porque, normalmente, o pensamento coletivo de resolver um problema da maneira mais ágil possível, acaba por comprometer a gestão da segurança da informação. Esta cultura precisa ser modificada antes da implantação de uma política. É preciso também efetuar um trabalho de convencimento de que a política de segurança não se trata apenas de burocratizar um processo ou regra de negócio, mas sim de implantar níveis de controle de modo que possam priorizar a garantia da confidencialidade, integridade e disponibilidade das informações.

É comum também enfrentarmos resistência por parte dos usuários ao iniciarmos um projeto de implantação de política de segurança. Tal resistência deve ser vencida através da conscientização, com exemplos práticos de danos à instituição pelo comprometimento de ativos.

Todos os integrantes da organização, desde a alta cúpula até o estagiário, devem ter ciência de que a informação é um dos ativos mais importantes com o qual eles irão lidar no dia a dia. A alta administração possui um papel fundamental neste processo, pois sem o seu envolvimento, dificilmente se conseguirá implementar uma política de segurança da informação. Iremos estudar mais adiante, no capítulo 5, os aspectos humanos da segurança da informação, no qual iremos detalhar as responsabilidades de cada classe de colaboradores, pois somente com a instrução e consciência de cada um, a política de segurança da informação poderá obter sucesso em seus variados aspectos.

1.5.1 Etapas para o desenvolvimento de uma política de segurança da informação

Ferreira e Araújo (2008) estabelecem quatro fases para o desenvolvimento e implementação das políticas, normas e procedimentos de segurança da informação em uma organização. Vamos conhecê-las?

- × **Fase 1: levantamento de informações** – nesta fase serão obtidas informações iniciais sobre os ambientes de negócios, ambiente tecnológico, bem como o entendimento das necessidades e uso dos recursos tecnológicos nos processos da instituição. Também serão agregados os padrões e normas já existentes na organização.
- × **Fase 2: desenvolvimento do conteúdo da política e normas de segurança** – fase que envolve aspectos como a classificação das informações (conforme estudamos no item 1.3), atribuição de regras e responsabilidades e, descrição de procedimentos que envolvem a TI como um todo, que vão desde a utilização dos recursos (e-mail, internet, software, entre outros) até o inventário dos ativos de informação.
- × **Fase 3: elaboração dos procedimentos de segurança da informação** – é nesta fase que serão formalizados os procedimentos levantados nas fases anteriores junto à alta administração. A formalização deve levar em conta as melhores práticas utilizadas no mercado e deve ser redigida de forma que possa ser integrada às políticas corporativas, levando em conta as necessidades e metas da organização.
- × **Fase 4: revisão, aprovação e implantação das políticas, normas e procedimentos de segurança da informação** – é a efetiva implantação das políticas, normas e procedimentos através de preparação de material promocional, divulgação constante, conscientização das responsabilidades, realização de palestras (em especial que envolva a alta cúpula) e palestras em linguagem simplificada, de modo que todo o público-alvo (colaboradores em geral) possa compreender e ser convencido a segui-las.

Importante

O executivo principal da organização deve atestar a política e exigir o cumprimento em todas as esferas da instituição. É necessário que ele demonstre o seu comprometimento em seguir as normas expostas no documento final redigido pela equipe responsável pela segurança da informação.

1.5.2 Divulgação, características e benefícios

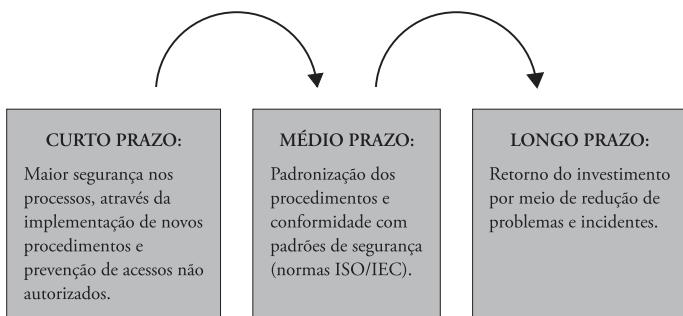
Sabemos que não é fácil modificar uma cultura dentro de um ambiente corporativo, ainda mais quando esta cultura inclui comportamentos e hábitos que comprometem a segurança das informações. Para que esta cultura seja modificada, é necessário que a empresa invista na conscientização e sensibilização de todos os funcionários. Isto pode ser feito por meio de avisos, palestras, elaboração de material promocional e treinamentos direcionados a áreas específicas, tais como, financeiro, RH, comercial, etc.

Sem dúvida, o elo mais fraco na corrente da segurança da informação é o elemento humano. Por mais que haja diversas tecnologias e metodologias para proteção das informações, se os funcionários não participam dos programas de treinamento e conscientização, comprometerão significativamente o sucesso da política. Por exemplo, quase todos os profissionais de Tecnologia da Informação já se deparamaram alguma vez com aquele usuário que escreve sua senha e cola no monitor!

Algumas características são fundamentais para que uma política obtenha sucesso na sua missão de garantir a confidencialidade, integridade e disponibilidade da informação. Ela deve, antes de tudo, ser verdadeira, no sentido de ser realista e coerente, de forma que seja possível o seu cumprimento. Também deve receber o aporte financeiro necessário e ser válida para todos. E finalmente ser simples, de modo que use uma linguagem de fácil compreensão, porém sem deixar de lado aspectos técnicos fundamentais.

Os benefícios alcançados com a correta implantação da política de segurança da informação variam de curto, passando por médio e chegando a longo prazo. A figura a seguir explica melhor quais são estes benefícios.

Figura 1.6 – Benefícios de uma política de segurança da informação



Fonte: Elaborada pelo autor (2016).

1.6 Atribuição de regras e responsabilidades

Segundo Ferreira e Araújo (2008, p. 70), “a responsabilidade pela preservação da segurança da informação e dos recursos que as produzem é de toda a organização”. Já citamos que o elo mais fraco da segurança da informação é o elemento humano, por isso é fundamental a participação de todos na proteção dos ativos de informação de uma organização. Todos devem ter consciência de seus papéis e responsabilidades neste processo. Ferreira e Araújo (2008) destacam as principais áreas que merecem nossa atenção durante a implantação de uma política de segurança da informação. Vamos conhecer algumas delas:

1.6.1 Comitê de segurança da informação

Já citamos que o envolvimento da alta cúpula de uma organização tem papel fundamental na implantação de uma política de segurança da informação. Os gestores devem elencar responsáveis de diversas áreas para compor um comitê que será responsável por estabelecer os procedimentos de segurança e traçar estratégias de divulgação destes procedimentos. Devem ser envolvidos profissionais das áreas de tecnologia, jurídico, financeira, administrativa, dentre outras.

O comitê deve ter a consciência de que uma vez estabelecida a política de segurança da informação, a mesma não pode ser engessada, mas deve acompanhar a evolução das regras de negócios da organização. Para tanto este comitê deve se reunir periodicamente ou sempre que julgar necessário, para atualizar os procedimentos adotados anteriormente.

O comitê deve promover o alinhamento dos objetivos de tecnologia da informação e dos objetivos institucionais com a segurança da informação. Deve ser o intermediador entre a alta cúpula e as áreas diversas do negócio, para a aprovação das políticas, normas e procedimentos de segurança da informação.

É importante que este comitê produza um relatório para a alta administração, contendo uma avaliação geral de todas as áreas, da efetividade dos sistemas de controle de segurança, com ênfase nos regulamentos, códigos internos e cumprimento das leis em vigor.

Saiba mais

Existem órgãos públicos da esfera federal que já possuem comitês de segurança da informação instaurados mediante legislação interna, como portarias e atos. Você pode consultar os documentos produzidos por um comitê acessando o sítio do Tribunal Regional do Trabalho da 11. região: <<http://governanca.trt11.jus.br/estrutura-de-ti/comite-de-seguranca-da-informacao-2/>>.

1.6.2 Proprietário das informações

É importante definir quem é o responsável direto pelas informações de uma determinada área de negócio. Ele deve ser um profissional com domínio de sua área de atuação. O proprietário também define quem terá acesso à informação, de acordo com as classificações já estudadas nos tópicos anteriores. Sugerimos iniciar a identificação dos proprietários pelos tipos de informações mais críticas ao negócio, por ser mais fácil a identificação deste tipo de informação. Cabe também ao proprietário a revisão periódica da classificação das informações.

1.6.3 Recursos humanos

É uma das áreas fundamentais, pois estabelecem as sanções e penalidades que devem ser aplicadas caso haja um descumprimento consciente de uma política de segurança da informação. A comunicação entre o RH e área de Tecnologia da Informação deve ser constante, em especial quando há desligamento de funcionários. Um funcionário desligado da empresa deve ter seu acesso aos sistemas e informações críticas imediatamente bloqueado, para evitar qualquer incidente de segurança, como por exemplo, uma vingança por motivação pessoal.

A área de RH também deve gerir a captura e guarda de Termos de Responsabilidade de Segurança da Informação. Todos os funcionários, estagiários e terceiros que ganhem acesso a informações críticas da organização

devem assinar um termo, responsabilizando-se pelo uso e não divulgação de informações classificadas.

1.6.4 Modelo de termo de responsabilidade de segurança da informação

Sua organização possui o hábito de solicitar ao funcionário, estagiário ou terceiro, que assine um **Termo de Responsabilidade de Segurança da Informação**? Esta é uma das maneiras pela qual as organizações podem resguardar-se em caso de violações e incidentes de segurança internos.

Apresentamos a seguir um exemplo simples de termo. Salientamos que o conteúdo pode variar de acordo com o tamanho da organização, processos internos e política de segurança da informação:

NOME DA EMPRESA

TERMO DE RESPONSABILIDADE DE SEGURANÇA DA INFORMAÇÃO

Política de Segurança da Informação

NOME COMPLETO, inscrito(a) no CPF sob o n. NNN, doravante denominado simplesmente FUNCIONÁRIO, em razão do seu vínculo com **NOME DA EMPRESA**, sito à **ENDEREÇO DA EMPRESA**, inscrita no CNPJ sob o n. NNN, doravante denominado EMPRESA, firma o presente TERMO DE RESPONSABILIDADE DE SEGURANÇA DA INFORMAÇÃO, mediante as estipulações consignadas neste instrumento:

a. O FUNCIONÁRIO declara expressamente, por este ato conhecer e assumir inteira responsabilidade pelo cumprimento das obrigações estabelecidas na Política de Segurança da Informação da EMPRESA;

b. Ter conhecimento de que:

I. A Política e as demais Normas de Segurança da Informação encontram-se disponíveis em **ENDEREÇO DA INTRANET** ou podem ser solicitadas no setor de Recursos Humanos ou de Tecnologia da Informação em caso de indisponibilidade.

- II. Todos os acessos efetuados, trabalhos desenvolvidos, informações manipuladas, arquivos, conteúdos, conexões, acesso remoto, mensagens eletrônicas e acesso a internet, podem ser verificados e auditados por funcionários da EMPRESA com atribuição para tal, a qualquer momento, independente de aviso prévio, podendo ainda revogar as autorizações que lhe tenham sido concedidas;
- III. Todos os ambientes físicos e lógicos da EMPRESA são monitorados para garantir a proteção e guarda das informações e dos Recursos de Tecnologia de Informação;
- IV. Não deverá publicar ou divulgar por qualquer meio, informações sigilosas que forem acessadas, obtidas ou geradas em decorrência das funções exercidas ou dos serviços contratados, sem permissão expressa da EMPRESA;
- V. As obrigações assumidas neste ato subsistirão permanentemente, mesmo após o término do vínculo do FUNCIONÁRIO com a EMPRESA, ou até que este comunique expressamente por escrito, que as informações já não são sigilosas;
- VI. Qualquer divulgação de informações sigilosas obtidas em razão do vínculo do FUNCIONÁRIO com a EMPRESA, sem autorização prévia, expressa e escrita, implica na obrigatoriedade de ressarcir as perdas e danos experimentados pela EMPRESA, sem prejuízo das penalidades civis e criminais previstas em lei.
- c. Este Termo tem natureza irrevogável e irretratável, vigorando a partir da data de sua assinatura.

E por estar de acordo com o inteiro teor deste Termo, o assina nesta data, para que produza seus jurídicos e legais efeitos.

CIDADE, DIA / MÊS / ANO

ASSINATURA DO FUNCIONÁRIO

Fonte: Adaptado de TJPE.

1.6.5 Responsabilidades

Para compreendermos melhor as responsabilidades, elaboramos o quadro a seguir. O domínio da segurança da informação é a área ou negócio principal com a qual a informação está relacionada. A responsabilidade primária é a área que tem como missão cumprir a política de segurança da informação, sendo assessorada pela área de apoio, especificada na terceira coluna.

Quadro 1.2 – Atribuição de responsabilidades

Domínios da Segurança da Informação	Responsabilidade Primária	Apoio
Política de segurança da informação	Segurança da informação	Comitê gestor de segurança da informação e departamento de comunicação interna
Organizando a segurança da informação	Segurança da informação	Gerência sênior, departamento de comunicação interna e auditoria interna
Gestão de ativos	Áreas de negócios	Segurança da informação e departamento jurídico
Segurança em recursos humanos	Recursos humanos	Segurança da informação
Segurança física e do ambiente	Gestor de facilidades (facilities)	Departamento de operações do data center
Controle de acesso	Gestor das unidades de negócios, segurança da informação e usuários individuais	Departamento de operação de rede
Aquisição, desenvolvimento e manutenção de sistemas de informação	Desenvolvimento de aplicações	Segurança da informação
Gestão de incidentes de segurança da informação	Segurança da informação	Peritos em investigação forense e departamento jurídico

Domínios da Segurança da Informação	Responsabilidade Primária	Apoio
Gestão de continuidade de negócios	Gestão de continuidade de negócios	Áreas de negócio e segurança da informação
Conformidade	Conformidade	Departamento jurídico

Fonte: Adaptado de Fagundes (2012).

1.7 Plano diretor de segurança

Até aqui estudamos diversos conceitos iniciais sobre a segurança da informação em um ambiente corporativo. Uma organização precisa decidir como irá se portar diante dos desafios que a segurança da informação impõe. Uma das formas mais práticas de fazer isso é elaborando um Plano Diretor de Segurança (PDS). Este plano tem como objetivo montar um mapa de relacionamento e dependência entre processos de negócio, aplicações e infraestrutura física, tecnológica e humana.

Como tais fatores apresentam volatilidade, o PDS deve ser dinâmico e flexível, adaptando-se às novas necessidades de segurança que venham a surgir no contexto corporativo. Cada corporação deve elaborar um plano compatível com suas necessidades, ameaças, vulnerabilidades e exposição ao risco, de modo que a corporação possa funcionar sob risco controlado e em nível tolerado.

Por mais que existam empresas com portes semelhantes e atuações de mercado compatíveis, não existe um modelo único de PDS capaz de atender todas as organizações de maneira uniforme. Por isso o PDS deve ser elaborado de acordo com cada particularidade. Lyra (2008) estabelece uma metodologia com seis etapas distintas e complementares para a elaboração deste plano, elencadas a seguir.

1.7.1 Identificação dos processos de negócios

O objetivo desta etapa é identificar, comumente por meio de entrevistas, os processos de negócios que serão alvos das próximas etapas. É de fundamen-

tal importância identificar quais são os processos mais sensíveis e mais críticos com base nos impactos financeiros e resultados estratégicos.

Nesta etapa também devem ser identificados os gestores-chaves dos processos mapeados, bem como promover a integração destes gestores com o intuito de obter sucesso na aplicação do plano diretor de segurança.

1.7.2 Mapeamento da relevância

Uma vez vencida a etapa de identificação dos processos de negócios, deve-se elencar, em ordem de prioridade, quais são os processos mais relevantes dentro da instituição. Pode ser uma tarefa difícil para quem não possua uma visão do todo, do funcionamento global da organização, portanto o envolvimento de gestores da alta administração é desejável para esta etapa.

Uma das formas de elencar este grau de relevância é atribuir uma nota, podendo ser de 1 a 5 (sendo 1 o nível menos relevante e 5 o nível mais relevante), quantificando assim a relevância do processo de negócio para a operação da organização.

1.7.3 Estudo de impactos (análise CIDAL)

Nesta etapa será identificada a sensibilidade de cada processo mapeado nas etapas anteriores, diante de um incidente de segurança. Os conceitos CIDAL – Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade serão estudados para cada um dos processos. A forma mais recomendada é através de entrevistas com os gestores-chaves de cada área. Em cada um destes processos deverá ser fornecida uma resposta pelos gestores dentro de cinco níveis: não considerável, relevante, importante, crítico e vital. O quadro 1.3 detalha os cinco níveis de impacto.

Quadro 1.3 – Níveis de impacto

Índice	Nível	Enquadramento
1	Não considerável	Quando um processo de negócio é afetado por um incidente de segurança e este incidente não representa prejuízo à atividade produtiva.

Índice	Nível	Enquadramento
2	Relevante	Quando um processo de negócio é afetado por um incidente de segurança e este incidente representa baixos impactos financeiros.
3	Importante	Quando um processo de negócio é afetado por um incidente de segurança e este incidente representa prejuízos financeiros diárias, sendo necessárias ações emergenciais a fim de que outros processos não venham a ser comprometidos.
4	Crítico	Quando um incidente de segurança afeta vários processos de negócios, causando prejuízos financeiros e operacionais de grande porte, sendo necessário ações reativas que afetam grande parte da organização.
5	Vital	Quando um incidente de segurança afeta todos os processos de negócios de uma organização e os danos causados são irreversíveis, podendo levar à falência da organização.

Fonte: Elaborada pelo autor.

1.7.4 Estudo de prioridades GUT

A próxima etapa é estabelecer uma prioridade para cada processo de negócio ameaçado, utilizando a matriz GUT: Gravidade (do problema), Urgência (da resolução do problema) e Tendência (do problema piorar). A matriz GUT também utiliza uma escala de 1 a 5, apresentada no quadro 1.4 que segue.

Quadro 1.4 – Matriz GUT

Gravidade	Urgência	Tendência
1 sem gravidade	1 sem pressa	1 não vai agravar
2 baixa gravidade	2 tolerante à espera	2 vai agravar a longo prazo

Gravidade	Urgência	Tendência
3 média gravidade	3 o mais cedo possível	3 vai agravar a médio prazo
4 alta gravidade	4 com alguma urgência	4 vai agravar a curto prazo
5 altíssima gravidade	5 imediatamente	5 vai agravar imediatamente

Fonte: Lyra (2008).

1.7.5 Estudo de perímetros

Nesta etapa serão identificados os ativos que sustentam e suportam os processos de negócio. Tais ativos pode ser pessoas, informações, aplicações, tecnologia e infraestrutura. O objetivo principal é mapear tudo o que está por trás do funcionamento do processo de negócio. Assim, uma vez identificados, passarão a fazer parte do plano diretor de segurança como ativos essenciais, bem como auxiliarão a mapear a relação entre estes ativos e os processos de negócio em análise.

1.7.6 Estudo de atividades

A etapa final do plano diretor de segurança consiste em elencar as atividades que irão complementar a implantação do PDS. Será necessário planejar as ações dos ambientes e perímetros distintos e isolados, mas que deverão estar alinhadas com as diretrizes de segurança da informação previamente definidas nas etapas anteriores. Como exemplo de áreas distintas podemos destacar: análise de códigos de aplicação, plano de resposta a invasões, capacitação em conceitos de segurança, testes de invasão e análise de riscos.

Síntese

Neste capítulo foi detalhado como a informação torna-se um dos ativos mais importantes de uma organização, visto que é necessário trabalhar dados brutos para obtê-la. Os conceitos aqui apresentados auxiliarão você a conscientizar os gestores de uma organização sobre a importância de proteger a informação e implementar uma política de segurança da informação que contemple todos os processos de negócio de uma empresa.

Você aprendeu os pilares da segurança da informação e a forma correta de classificar a mesma de acordo com critérios bem consolidados no ambiente corporativo atual. Agora que você já conhece estes conceitos, podemos avançar no estudo da segurança da informação e auditoria de sistemas, conhecendo mais a fundo as normas de segurança e boas práticas que todas as organizações deveriam conhecer.

Atividades

1. Explique, resumidamente, a diferença entre dados, informação e conhecimento.
2. Cite quais são os pilares, bem como os conceitos complementares, bases da Segurança da Informação
3. O ciclo de vida da informação é a etapa mais importante de todo processo de gestão da informação, pois dentro de suas finalidades básicas de conhecimento dos ambientes interno e externo da organização e atuação nesses ambientes, é ela que garante melhores resultados em uma organização. Trata-se da etapa de: (Questão de concurso público MPE/RN 2010 - 2010 - Analista de TI - Suporte Técnico)
 - a) Obtenção.
 - b) Uso.

- c) Tratamento.
 - d) Distribuição.
 - e) Armazenamento.
4. Analise a frase a seguir. A classificação da informação como “confidencial” caracteriza-se por ser exclusiva do ambiente interno e de forma muito controlada, somente pessoas específicas devem ter acesso à informação. Sua divulgação trará alto impacto à organização.
- a) Certo
 - b) Errado

2

Metodologias e Padrões de Segurança da Informação

DURANTE AS DÉCADAS em que a Tecnologia da Informação ganhou cada vez mais espaço dentro das corporações, foi preciso estabelecer uma série de normas e regras que pudessem auxiliar os gestores a prover meios capazes de garantir a segurança da informação. Neste capítulo iremos conhecer as principais normas e padrões de segurança da informação, cujo objetivo é definir regras, critérios, princípios e melhores práticas, a fim de que haja uniformidade nos processos, produtos ou serviços de uma organização. Você irá conhecer em detalhes as principais normas da família ISO/IEC 27001, bem como os conceitos principais do COBIT e ITIL, a fim de que seja capaz de auxiliar uma organização a implementar as melhores práticas de segurança da informação adotadas mundialmente.

Objetivo de aprendizagem:

- × Compreender a aplicação e funcionamento das principais normas e padrões adotados para segurança da informação.

2.1 Introdução às normas e padrões

Nos dias de hoje são muitas as normas existentes no mercado corporativo, cada qual possuindo seu escopo e objetivo bem definidos. As normas relacionadas às áreas de Tecnologia da Informação existem devido à dificuldade destas áreas em manterem seus próprios modelos e estruturas de controle, uma vez que as evoluções tecnológicas criam constantes necessidades de atualizações destes modelos. Estudaremos neste capítulo as normas relacionadas mais especificamente com a segurança da informação.

Abordaremos as normas NBR ISO/IEC 27001, NBR ISO/IEC 27002, COBIT e ITIL ao longo do capítulo. Porém, antes de avançarmos no estudo destas normas, vamos compreender como são formadas estas siglas que compõem os nomes destas normas.

A ISO é uma entidade de padronização e normatização de alcance global, fundada em Genebra, na Suíça, no ano de 1947. Seu nome original é *International Organization for Standardization*, que em português significa Organização Internacional para Padronização. Apesar da ordem das letras não ser idêntica para cada língua e, como em cada país acabaria existindo uma sigla diferente para a organização, os fundadores decidiram escolher uma só sigla para todos os países: ISO. Seu objetivo principal é aprovar normas internacionais em todos os campos técnicos.

De forma a reunir diversas normas de segurança da informação, a ISO criou a série 27000. Esta família é composta por dezenas de normas relacionadas à segurança da informação (ISO, 2016), porém nosso estudo abrangerá as duas principais e mais amplamente utilizadas no mercado: 27001 e 27002.

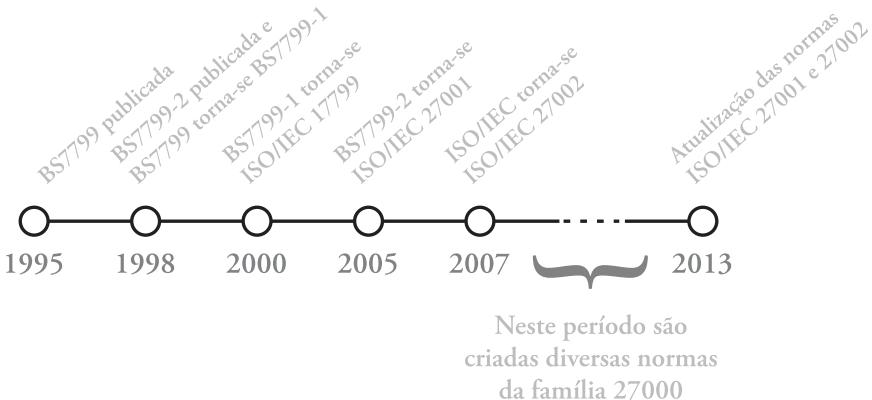
No Brasil, a ABNT (Associação Brasileira de Normas Técnicas) oferece a tradução literal das normas ISO, acrescentando assim a sigla NBR antes do nome da norma.

A padronização para a área de segurança da informação foi iniciada pelo BSI (*British Standard Institute*) com a criação da norma BS7799 na década

de 1990, sendo considerado o mais completo padrão para o gerenciamento da segurança da informação no mundo. Esta publicação tornou possível a implantação de um sistema de gestão de segurança baseado em controles definidos por uma norma e prática internacional.

Na figura a seguir podemos ver a linha do tempo da evolução das normas em questão:

Figura 2.1 – Evolução das normas da família 27000



Fonte: Adaptado de www.iso.org.

2.2 Comparativo entre as normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002

Antes de avançarmos no estudo destas normas é importante compreendermos qual o escopo e abrangência de cada uma delas. Cada uma das normas possui um foco determinado. Em uma análise inicial percebe-se que a norma 27002 possui uma grande riqueza de detalhes. Para que uma empresa possa construir os alicerces de segurança da informação, definindo suas estruturas, deve-se utilizar a ISO 27001. A organização que dela se utiliza passa a reduzir o risco de responsabilidades pela não implantação ou determinação de políticas e procedimentos de segurança da informação. Uma das vantagens desta norma é que a alta administração passa a assumir a responsabilidade pela segurança da informação. Já a ISO 27002 possui um nível de detalha-

mento muito mais amplo, fornecendo um conjunto de controles baseados em melhores práticas para a segurança da informação, servindo como um guia para áreas mais específicas. As normas, portanto, se complementam e foram separadas por uma questão de usabilidade, pois se fossem uma única norma ela seria muito complexa e grande para uma aplicação prática.

2.3 NBR ISO/IEC 27001:2013

O objetivo desta norma é prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Um SGSI é um sistema, não necessariamente informatizado, que tem por objetivo ser um conjunto de processos e procedimentos, baseado nas normas e legislação vigentes, voltados à proteção de ambientes que criam, utilizam-se ou descartam informações relevantes. Ferreira e Araújo (2008, p. 54) definem o SGSI como “o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação”. Na prática, quando uma instituição implanta a norma ISO 27001, acaba por constituir um SGSI.

Implementar um SGSI é uma escolha estratégica para uma organização. A concepção e implementação do SGSI é influenciada pelos objetivos de negócio, segurança, riscos, requisitos de controle, processos empregados e o tamanho e estrutura da organização, ou seja, uma necessidade simples requer uma solução simples de SGSI.

A análise dos requisitos para a proteção de ativos de informação e a aplicação de controles adequados para garantir a proteção destes ativos contribui para a implementação bem-sucedida de um SGSI. Listamos também alguns aspectos que contribuem para tal:

- a) consciência da necessidade de segurança da informação;
- b) atribuição de responsabilidade pela segurança da informação;
- c) avaliações de risco que determinem os controles apropriados para atingir níveis aceitáveis de risco;

- d) segurança incorporada como elemento essencial das redes e sistemas de informação;
- e) prevenção ativa e detecção de incidentes de segurança da informação;
- f) assegurar uma abordagem global da gestão da segurança da informação;
- g) reavaliação contínua da segurança da informação e modificações, conforme apropriado.

2.3.1 Importância de um SGSI dentro de uma organização

Em um mundo interconectado, a informação e processos, sistemas e redes relacionados constituem ativos críticos da empresa, como já estudamos no capítulo 1. As organizações e seus sistemas de informação enfrentam ameaças constantes à segurança de uma ampla gama de fontes, incluindo invasão a sistemas computacionais, espionagem, sabotagem, vandalismo, incêndio e inundações. Danos a sistemas de informação e redes causados por códigos maliciosos, hackers e os ataques de negação de serviço tornaram-se mais comuns, mais ambiciosos e cada vez mais sofisticados.

A implantação de um SGSI pode contribuir muito para a garantia da reputação de uma organização. Embora não seja o único fator para tal, demonstrará para clientes, fornecedores e colaboradores que a segurança da informação é fundamental na operação da empresa.

A adoção de um SGSI é uma decisão estratégica para uma organização e é necessário que essa decisão seja integrada, dimensionada e atualizada de acordo com as necessidades desta. A obtenção de segurança da informação requer a gestão do risco e engloba os riscos das ameaças físicas, humanas e tecnológicas associadas a todas as formas de informação dentro ou utilizadas pela organização.

A concepção e implementação do SGSI de uma organização é influenciada pelas necessidades e objetivos da organização, pelos requisitos de segurança, pelos processos de negócio utilizados e pelo tamanho e estrutura da organização. A concepção e o funcionamento de um SGSI devem refletir os

interesses e os requisitos de segurança da informação de todas as partes interessadas da organização, incluindo clientes, fornecedores, parceiros de negócios, acionistas e outros terceiros relevantes.

Um SGSI é de fundamental importância para empresas do setor público e privado. A interconexão de redes públicas e privadas e o compartilhamento de ativos de informação aumenta a dificuldade de controlar o acesso e o tratamento da informação. Além disso, a distribuição de dispositivos de armazenamento, como *pendrives*, pode enfraquecer a eficácia dos controles tradicionais. Quando as organizações adotam a família de padrões do SGSI, a capacidade de aplicar princípios de segurança de informação pode ser demonstrada aos parceiros de negócios e a outras partes interessadas.

A segurança da informação nem sempre é levada em conta na concepção e desenvolvimento dos sistemas de informação. Além disso, a segurança da informação é muitas vezes considerada como uma solução técnica. No entanto, a segurança da informação que pode ser alcançada por meio de meios técnicos é limitada e pode ser ineficaz sem ser apoiada por uma gestão e procedimentos adequados no contexto de um SGSI.

Integrar a segurança em um sistema corporativo pode ser difícil e dispendioso. Um SGSI envolve um planejamento cuidadoso e atenção aos detalhes. Como exemplo, os controles de acesso, que podem ser técnicos (lógicos), físicos, administrativos (gerenciais) ou uma combinação destes, fornecem um meio para garantir que o acesso a ativos de informações seja autorizado e restrito com base nos requisitos de segurança (tríade CID) de negócios e informações.

2.3.2 Abordagem Plan-Do-Check-Act (PDCA)

A norma NBR ISO/IEC 27001 adota o modelo conhecido como *Plan-Do-Check-Act* (PDCA). O ciclo PDCA é a metodologia mais utilizada para implementar um sistema de melhoria contínua em uma empresa ou organização. O nome PDCA é também conhecido como o Ciclo de Melhoria Contínua ou *Deming Cycle* (devido ao nome de seu idealizador, Edwards Deming). Esta metodologia descreve as quatro etapas essenciais que devem ser realizadas sistematicamente para alcançar a melhoria contínua, definida como uma forma contínua de melhorar a qualidade de nossos produtos e

processos (diminuição de falhas, aumento da eficácia e eficiência, resolução de problemas, prevenção de riscos potenciais etc).

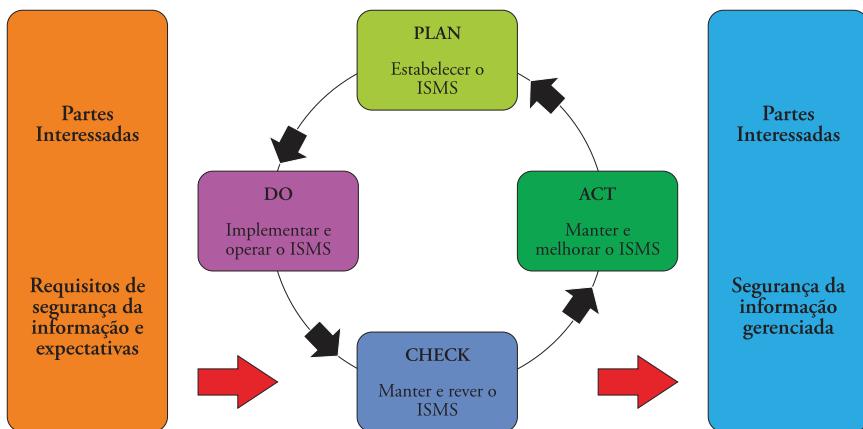
O Ciclo de Deming é composto por quatro etapas cíclicas, de modo que uma vez terminado o estágio final temos que começar novamente com o primeiro, e repetir o ciclo novamente. Fazendo isso em uma empresa, as atividades são reavaliadas periodicamente para incorporar novos aprimoramentos. A seguir explicaremos cada parte do ciclo PDCA, para uma melhor compreensão sobre as interações dos ciclos com a implementação do SGSI em uma organização.

- × **Plan:** localizar o que pode ser melhorado, fixar um objetivo e avaliar como este objetivo pode ser alcançado. É recomendado criar grupos de trabalho para pesquisar melhorias potenciais nos processos e produtos da organização. Isto auxilia a receber ideias dos funcionários, e a encontrar melhores e novas tecnologias que a empresa ainda não usou;
- × **Do:** nesta etapa são realizadas as mudanças necessárias para implementar a melhoria proposta nos processos. Em geral, recomenda-se fazer um projeto piloto para testar a operação antes de fazer mudanças em larga escala;
- × **Check:** uma vez que as mudanças são implementadas, é estabelecido um período experimental para verificar o desenvolvimento do novo processo. Se a melhoria não atingir as expectativas iniciais, será necessário modificar o processo novamente para alcançar os objetivos desejados;
- × **Act:** na etapa final, quando o período experimental termina, é preciso estudar os resultados e comparar o desempenho dos processos e atividades antes e depois da melhoria. Se os resultados forem satisfatórios, as melhorias serão implementadas permanentemente. No entanto, se eles não forem satisfatórios, deve-se decidir entre fazer mais mudanças para ajustar os resultados ou descartá-los e retornar ao ponto inicial.

Entre as vantagens de utilizar a metodologia destacamos a possibilidade de fornecer um método padronizado para alcançar a melhoria contínua que

pode ser usado por funcionários em qualquer departamento para resolver novos e recorrentes problemas. Além disso, também pode representar baixo custo de implementação (os obstáculos são superados internamente), bem como evitar desperdício de tempo implementando soluções ineficazes ou inferiores. A figura 2.2 apresenta a abordagem PDCA alinhada à implementação de um SGSI.

Figura 2.2 – Abordagem *Plan-Do-Check-Act* (PDCA)



Fonte: Elaborada pelo autor.

O quadro 2.1 apresenta o detalhamento de cada etapa PDCA alinhada à implementação de um SGSI:

Quadro 2.1 – Ciclo PDCA, implementação de um Sistema de Gestão de Segurança da Informação

Fase 1 <i>Plan</i> (planejar)	Fase 2 <i>Do</i> (fazer)	Fase 3 <i>Check</i> (checar)	Fase 4 <i>Act</i> (agir)
Estruturação do SGSI	Comitê de segurança da informação	Monitoração dos controles de segurança	Implementação de melhorias
Plano diretor de segurança	Política de segurança	Gestão de incidentes	Ações corretivas e preventivas

Fase 1 <i>Plan</i> (planejar)	Fase 2 <i>Do</i> (fazer)	Fase 3 <i>Check</i> (checkar)	Fase 4 <i>Act</i> (agir)
Diagnóstico de segurança	Classificação das informações	Revisão do nível de risco residual	Comunicação das ações e resultados para a alta administração e partes interessadas
Avaliação, tratamento dos riscos e seleção dos controles de segurança	Plano de continuidade de negócios e de TI	Auditória interna do SGSI	Assegurar que as melhorias foram implementadas e atenderam as expectativas
Declaração de aplicabilidade (<i>statement of applicability</i>)	Treinamento e conscientização		
	Implementação dos controles específicos na declaração de aplicabilidade		

Fonte: Ferreira; Araújo (2008).

2.3.3 Certificação NBR ISO/IEC 27001:2013

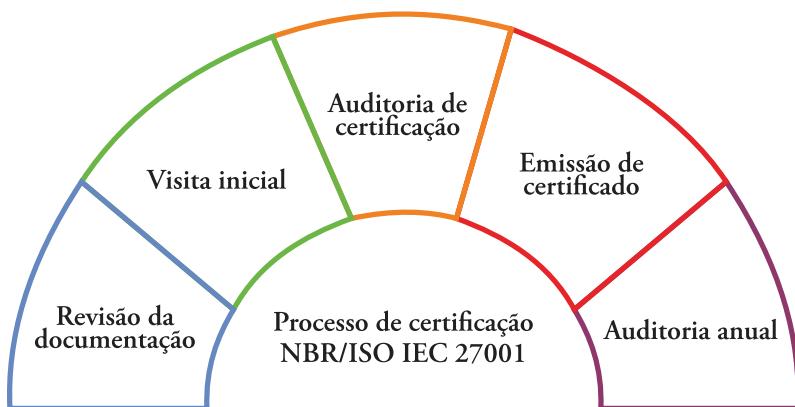
Atualmente existem profissionais atuantes no mercado brasileiro com equipes de auditores e consultores capacitados para a preparação das empresas que desejam obter a certificação ISO 27001. Por questões éticas, a empresa que presta consultoria no processo de preparação não efetua a auditoria de certificação.

As empresas que optam pela certificação passam a valer-se de vários benefícios, como redução de prêmios de seguro, diferencial competitivo diante de investidores, e também como um atestado público de capacidade, efetuando

uma demonstração pública do compromisso da empresa com a segurança das informações de seus clientes.

A figura a seguir detalha as etapas resumidas do processo de certificação.

Figura 2.3 – Processo de certificação NBR ISO/IEC 27001



Fonte: Adaptado de Ferreira e Araújo (2008).

A etapa de **revisão de documentação** consiste da verificação do sistema de gestão de segurança da informação em compatibilidade com as normas ISO 27001 e ISO 27002. A próxima etapa é a **visita inicial**, na qual serão levantadas informações gerais antes da auditoria e definição do escopo. É importante frisar que o escopo é definido nos termos das características do negócio da organização e devem ser incluídos detalhes e justificativas para quaisquer exclusões do escopo.

Após esta etapa, procede-se a **auditoria de certificação**, em que serão realizadas entrevistas e análise do SGSI em operação. Caso tudo esteja em conformidade com a norma, é emitido o **certificado**. E para que a empresa possa manter a certificação, serão realizadas **auditorias anuais**, a fim de verificar se o SGSI continua operando satisfatoriamente.

2.3.4 Tópicos da NBR ISO/IEC 27001:2013

A norma apresenta-se com os seguintes tópicos:

- ✖ **escopo** – descreve os objetivos gerais e a aplicação da norma, fundamentalmente voltados à implementação de um SGSI.
- ✖ **referência normativa** – referência indispensável para a aplicação da norma.
- ✖ **termos e definições** – apresenta um glossário completo com termos técnicos fundamentais.
- ✖ **contexto da organização** – apresenta tópicos sobre a organização e seu contexto, entendendo as necessidades e expectativas das partes interessadas, bem como a determinação do escopo do sistema de gestão da segurança da informação.
- ✖ **liderança** – detalha a necessidade do comprometimento da alta administração da organização, bem como papéis e responsabilidades.
- ✖ **planejamento** – engloba desde avaliação e tratamento de riscos bem como o objetivo de segurança da informação e planejamento para alcançá-lo.
- ✖ **apoio** – detalha as áreas e ações de apoio.
- ✖ **operação** – trata do planejamento operacional, englobando novamente avaliação e tratamento de riscos.
- ✖ **avaliação de desempenho** – contempla as etapas de monitoramento, medição, análise e avaliação, bem como auditoria interna e análise crítica por parte da alta administração.
- ✖ **melhoria** – incentiva a melhoria contínua por meio de constantes ações corretivas.

Importante

A norma possui ainda um anexo denominado “Anexo A”, que possui controles com os mesmos nomes dos controles da norma ISO 27002. A diferença está no nível de detalhamento, em média a ISO 27002 utiliza-se de uma página inteira para explicar um controle, enquanto a ISO 27001 dedica apenas uma frase para cada controle.

2.4 NBR ISO/IEC 27002:2013

A norma ISO 27002 funciona em alinhamento com a ISO 27001. Citamos no tópico anterior que os controles presentes no Anexo A da ISO 27001 são detalhados na ISO 27002. Para que uma organização possa implementar um sistema de gestão da segurança da informação (SGSI) baseada na ISO 27001, ela necessita de um documento de orientação para a efetiva implantação dos controles de segurança da informação comumente aceitos.

As normas ISO 27002 são um código de prática para a segurança da informação que descrevem todos os potenciais controles e mecanismos de controle que podem teoricamente ser implementados, com a orientação fornecida pela ISO 27001. As organizações são livres para selecionar e implementar controles alternativos e ignorar qualquer um dos controles, mas se uma organização optar por não adotar algo tão básico como, por exemplo, uma boa solução de antivírus, elas devem estar preparadas para justificar a sua decisão.

O objetivo principal da ISO 27002 é fornecer um programa de gerenciamento de segurança de informações abrangente para qualquer organização que necessite de um novo programa de gerenciamento de segurança de informações ou queira melhorar suas políticas e práticas de segurança de informação existente. A norma fornece as recomendações para gerenciar a segurança da informação para as pessoas que são responsáveis por iniciar, implementar e manter a segurança da informação em qualquer organização. A ISO/IEC recomenda que cada organização considere cada uma dessas práticas quando estabelecerem ou melhorarem o programa de gerenciamento de segurança da informação de sua organização. No entanto, como cada empresa tem um conjunto único de riscos de segurança da informação, bem como seus requisitos, ela pode escolher as práticas de segurança da informação de acordo com seus próprios requisitos de segurança e ignorar os que não se aplicam a elas.

A segurança da informação é um tema amplo e, portanto, a ISO 27002 tem aplicabilidade em todos os tipos de organizações, incluindo empresas comerciais de todos os tamanhos, organizações sem fins lucrativos, órgãos governamentais, instituições de caridade e qualquer outra organização que lida e depende de informações.

2.4.1 Certificação NBR ISO/IEC 27002:2013

A certificação ISO 27002 é voltada para profissionais que desejam atuar no mercado de segurança da informação. A prova de certificação testa o profissional para o conhecimento sobre um sistema de gerenciamento da segurança da informação. Este profissional atua junto a empresas que desejam obter a certificação empresarial ISO 27001 (detalhada no tópico 2.3.3).

Saiba mais

O exame de ISO 27002 é composto por 40 questões de múltipla escolha, onde o candidato deve acertar no mínimo 26 questões (65%) para passar no exame e com um tempo de duração de 1 hora.

O exame está disponível também em português.

2.4.2 Tópicos da NBR ISO/IEC 27002:2013

A norma é dividida em tópicos, os quais detalhamos:

- × **introdução e escopo** – são explicados os objetivos gerais e a aplicação da norma, fundamentalmente voltados a práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, implementação e o gerenciamento de controles.
- × **referências normativas** – referências indispensáveis para a aplicação da norma.
- × **termos e definições** – constitui-se de um glossário completo com termos técnicos fundamentais.
- × **políticas de segurança da informação** – apresentam como objetivo a divulgação de normas que visam apoiar a alta administração a implementar a segurança da informação, obedecendo a normas e regulamentos em vigor, respeitando também os requisitos de negócio.

- × **organização da segurança da informação** – orienta como estabelecer uma estrutura de gerenciamento, para iniciar e controlar a implementação da segurança da informação dentro da organização.
- × **segurança em recursos humanos** – o objetivo desta seção é orientar os funcionários e partes externas que interagem com a organização, de modo que todos entendam suas responsabilidades no processo da segurança da informação como um todo.
- × **gestão de ativos** – engloba a identificação dos ativos da organização e define as responsabilidades apropriadas para a proteção dos mesmos.
- × **controle de acesso** – estabelece os limites de acesso à informação e aos recursos de processamento da informação.
- × **criptografia** – nesta seção são abordados aspectos de orientação para assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.
- × **segurança física e do ambiente** – o acesso físico às instalações e à infraestrutura de apoio (comunicações, energia, ar condicionado, etc.) deve ser monitorizado e restrito para prevenir, detectar e minimizar os efeitos do acesso não autorizado e inapropriado.
- × **segurança das operações** – tem como objetivo orientar quanto aos procedimentos e responsabilidades para a garantia da operação segura dos recursos de processamento da informação, tais como: proteção contra *malware*, backup, registro e monitoramento, controle de software operacional e gerenciamento técnico de vulnerabilidades.
- × **segurança nas comunicações** – detalha a garantia da proteção das informações em redes e dos recursos de processamento da informação que os apoiam.
- × **aquisição, desenvolvimento e manutenção de sistemas** – evidencia que é necessário garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação, incluindo também os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.

- ✖ **relacionamento com fornecedor** – também denominado “relacionamento na cadeia de suprimento”, visa garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores.
- ✖ **gestão de incidentes de segurança da informação** – tem como objetivo assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.
- ✖ **aspectos da segurança da informação na gestão da continuidade do negócio** – identifica os aspectos que devem ser observados em situações adversas, como por exemplo durante uma crise ou desastre. Convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação nestas situações.
- ✖ **conformidade** – orienta quanto aos procedimentos a fim de evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

2.5 COBIT

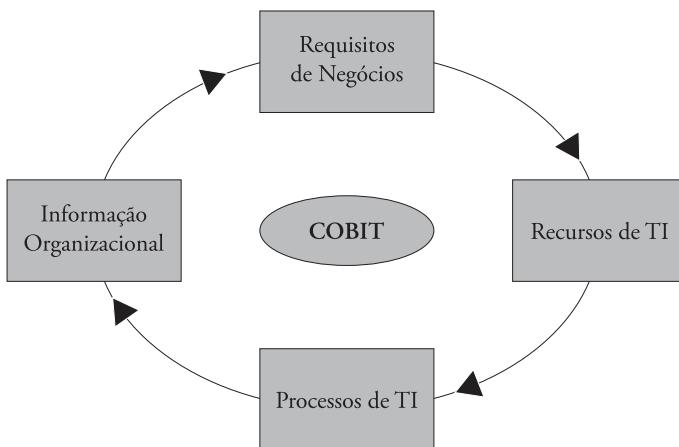
COBIT é um acrônimo para *Control Objectives for Information and Related Technology*, na tradução para o português significa “Objetivos de Controle para Tecnologia da Informação e Áreas Relacionadas”. O COBIT é baseado em controles, para servir como referência a uma organização que deseja ter uma governança de TI mais controlada. É focado no negócio e orientado a processos sendo necessário adaptá-lo ao negócio para atender às necessidades de uma organização. Atualmente encontra-se na versão 5.

O COBIT é mantido por uma entidade independente e sem fins lucrativos denominada ISACA (*Information Systems Audit and Control Association*), cujo objetivo é desenvolver padrões internacionais de controle e auditoria de sistemas da informação, que ajudam seus usuários a garantir a confiança e o valor dos mesmos.

Em diversas organizações a área de Tecnologia da Informação possui um funcionamento de modo independente à empresa na qual está inserida,

muitas vezes tornando difícil para a alta administração compreender, por exemplo, como os investimentos aplicados nesta área ajudam a organização a atingir seus objetivos e suas metas. O COBIT procura atender esta e outras necessidades, de modo a guiar os investimentos na área de TI, analisando os riscos e atendendo a legislação pertinente. Voltado para esta perspectiva, os investimentos de TI são guiados pelas necessidades do negócio, sendo usados em processos de TI que entregam algum valor de volta à organização, respondendo aos requisitos de negócios que criaram o ciclo. A figura a seguir exemplifica este ciclo:

Figura 2.4 – Alinhamento de TI e negócios



Fonte: Adaptada de www.isaca.org.

As estruturas de controles contidos no COBIT são aceitas mundialmente como as melhores praticados para o estabelecimento da segurança para a área de TI, em empresas de diversos ramos de negócio, em especial, do setor financeiro.

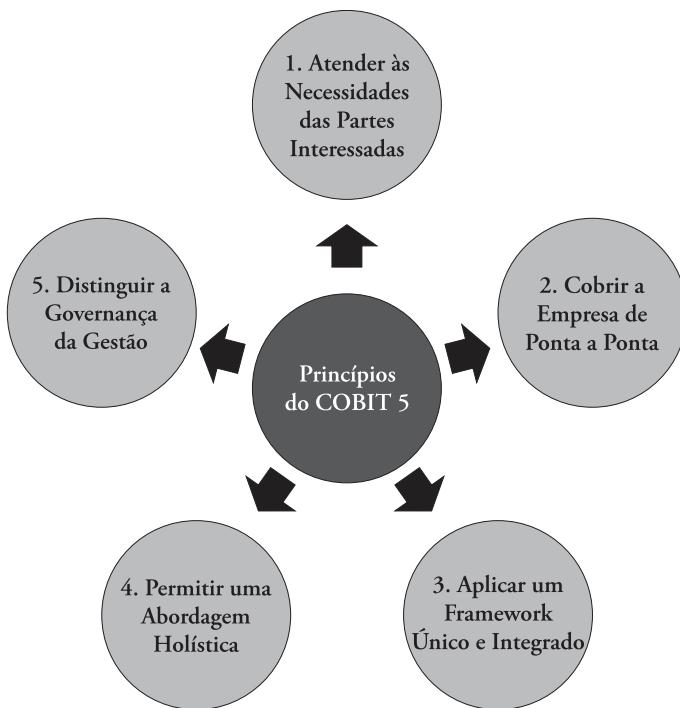
As empresas e organizações, em especial a alta administração, devem reconhecer que a TI é tão significativa para os negócios como qualquer outra parte da organização, sendo este um fator crucial para o seu sucesso. Diretores e gestores devem colaborar e trabalhar em conjunto a fim de garantir que a TI esteja inclusa na abordagem de governança e gestão, devido a importância da TI que deixou de atuar simplesmente no papel de suporte e passou a assumir

uma posição central dentro das empresas. Além disso, cada vez mais leis e regulamentos estão sendo aprovados e estabelecidos para atender a essa necessidade. O COBIT fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI.

2.5.1 Princípios do COBIT

O COBIT, em sua versão 5, baseia-se em 5 princípios básicos para governança e gestão de TI da organização, apresentados na figura a seguir:

Figura 2.5 – Princípios do COBIT



Fonte: ISACA (<http://www.isaca.org>).

- Atender às necessidades das partes interessadas:** este princípio define que os *stakeholders* (também denominados partes interessadas, que são pessoas ou grupos que possuem investimento ou

interesse em um determinado negócio) estão tornando-se o foco das organizações nos últimos tempos. A entrega do valor às partes interessadas da empresa requer boa governança e gerenciamento de ativos de Tecnologia da Informação. O COBIT descreve os processos necessários (e outros facilitadores) para apoiar a criação de valor por meio do uso de TI e permite transformar as necessidades das partes interessadas em uma estratégia alcançável. A cascata de metas do COBIT é o mecanismo usado para traduzir essas necessidades em metas empresariais personalizadas. Este mapeamento de necessidades é a chave para apoiar o alinhamento entre as necessidades de uma empresa e soluções e serviços de TI, e pode ser aplicado em vários níveis.

- b) Cobrir a empresa de ponta a ponta:** o COBIT aborda a governança e o gerenciamento de informações e tecnologias relacionadas de uma perspectiva corporativa de ponta a ponta. Isto significa integrar a governança de TI corporativa na governança corporativa, ou seja, o sistema de governança para TI empresarial proposto pelo COBIT integra-se perfeitamente em qualquer sistema de governança porque o COBIT alinha-se com as últimas visões sobre governança. Abrangendo todas as funções e processos dentro da empresa e não se concentrando apenas na função de TI, o COBIT trata a informação e tecnologias relacionadas como ativos que precisam ser tratados como qualquer outro ativo por todos na empresa.
- c) Aplicar um modelo (*framework*) único e integrado:** como existem muitas normas e boas práticas relacionadas a TI, O COBIT procura alinhar-se a outros padrões e modelos importantes, como as normas da família ISO 27000 e ITIL (que abordaremos no tópico 3.5). Sendo assim, pode servir como um modelo unificado para a governança e gestão de TI da organização.
- d) Permitir uma abordagem holística:** o quarto princípio explica que a governança eficiente e eficaz e a gestão de TI empresarial requerem uma abordagem holística, levando em consideração vários componentes que interagem entre si, sejam processos, estruturas e pessoas. O COBIT define um conjunto de facilitadores que auxi-

liam a implementação de um sistema abrangente de governança e gerenciamento para TI empresarial. Os facilitadores são tem como função ajudar a alcançar os objetivos da empresa. O *framework* COBIT define sete categorias destes, sendo: princípios, políticas e modelos; processos; estruturas organizacionais; cultura, ética e comportamento; informação; serviços, infraestrutura e aplicativos; pessoas, habilidades e competências.

- e) **Distinguir a governança da gestão:** o princípio estabelece distinção clara entre governança e gestão. A governança garante que as necessidades, condições e opções das partes interessadas são avaliadas para determinar objetivos de negócios equilibrados e acordados a serem alcançados. Isso significa que a governança deve monitorar o desempenho, a conformidade e o progresso de acordo com a direção e os objetivos acordados. Uma das principais responsabilidades da governança é avaliar, direcionar e monitorar.

A gestão, por outro lado, planeja, constrói, executa e monitora atividades para alinhar e apoiar os objetivos de governança. Governança é uma responsabilidade do conselho, enquanto a gestão é uma responsabilidade da gerência executiva. Estruturas não são normas e podem ser modificadas para atender às necessidades da maioria das organizações, desde que haja a separação necessária entre governança e gestão. Sem essa separação, há risco com relação a responsabilidades em diferentes níveis.

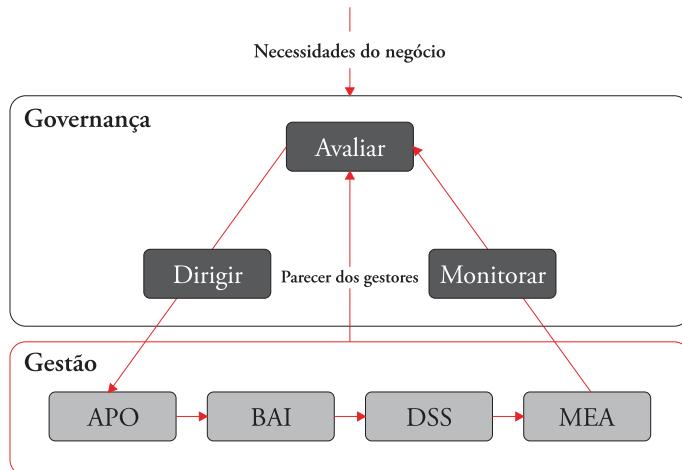
Saiba mais

Governança de TI é um braço da governança corporativa. De acordo com o TCU, "É um conjunto estruturado de políticas, normas, métodos e procedimentos destinados a permitir à alta administração e aos executivos o planejamento, a direção e o controle da utilização atual e futura de tecnologia da informação. De modo a assegurar, a um nível aceitável de risco, eficiente utilização de recursos, apoio aos processos da organização e alinhamento estratégico com objetivos desta última. Seu objetivo, pois, é garantir que o uso da TI agregue valor ao negócio da organização."

2.5.2 Modelo de referência de processos do COBIT

O modelo de referência de processos do COBIT, versão 5, seguindo a lógica de um dos seus cinco princípios, subdivide os 37 processos de TI em duas principais áreas de atividade: Governança e Gestão. Por sua vez, estas duas áreas são divididas em domínios de processos, conforme apresentado na figura 2.6.

Figura 2.6 – Áreas chave de governança e gestão



Fonte: Adaptado de www.isaca.org.

Os processos de **governança** estão inseridos em um domínio “Avaliar, Dirigir e Monitorar” (EDM), sendo que este domínio contém 5 processos de governança. Esses processos definem as responsabilidades da diretoria para avaliar, direcionar e monitorar o uso de ativos de TI a fim de criar valor para a empresa. O domínio EDM abrange a definição da estrutura de governança, estabelecendo responsabilidades em termos de valor, fatores de risco e recursos, mantendo a transparéncia de TI para as partes interessadas.

Os processos de gestão contêm quatro domínios, de acordo com as áreas detalhas a seguir. Estes domínios são uma evolução da estrutura de domínios e processos do COBIT 4.1:

- × **Alinhar, Planejar e Organizar (APO)** – o domínio APO contém 13 processos, os quais abrangem o uso de informações e tecnologia

e a melhor maneira de utilizá-las para ajudar a atingir os objetivos e metas da empresa. Destaca também a forma organizacional e infraestrutura que a TI deve ter para alcançar os melhores resultados e gerar os maiores benefícios de seu uso.

- ✖ **Construir, Adquirir e Implementar (BAI)** – o domínio BAI contém 10 processos, visando criar, adquirir e implementar domínios que identificam os requisitos de TI, investindo na tecnologia e a implementação desta dentro dos processos de negócios atuais da empresa.
- ✖ **Entregar, Servir e Suportar (DSS)** – o domínio DSS contém 6 processos, os quais se referem à entrega dos serviços de TI necessários para atender aos planos táticos e estratégicos.
- ✖ **Monitorar, Avaliar e Medir (MEA)** – o domínio MEA contém 3 processos. Seu objetivo é monitorar o desempenho dos processos de TI, avaliando a conformidade com os objetivos e com os requisitos externos.

2.6 ITIL

O padrão atual da indústria para implantar o gerenciamento de serviços de TI é a biblioteca de infraestrutura de TI, *IT Infrastructure Library* (ITIL). Esta biblioteca teve início nos anos 1980, quando o governo britânico percebeu a necessidade de melhorar os seus serviços de TI. A tarefa de desenvolver um arcabouço para usar os recursos de TI de maneira financeiramente responsáveis e eficiente foi dada ao *Office of Government Commerce (OGC)*. A ITIL foi rapidamente adotada por outros governos e grandes empresas da Europa. Atualmente a ITIL encontra-se na sua terceira versão, lançada em 2007, embora em 2011 tenha ocorrido uma atualização para corrigir erros, remover inconsistências e melhorar a clareza e a estrutura.

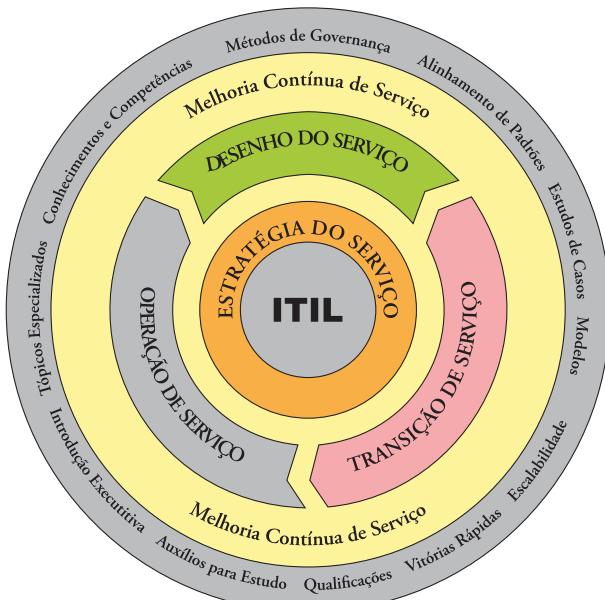
2.6.1 Organização

A ITIL organiza os processos para o gerenciamento dos serviços de TI por meio de um ciclo de vida de serviços. No total a ITIL define 26 processos e 4 funções para o gerenciamento de serviços. A ITIL é descrita em dois componentes básicos:

- × **núcleo do ITIL** – é onde se encontram as orientações sobre as melhores práticas aplicáveis a todos os tipos de organizações que prestam serviços ao negócio.
- × **guias complementares do ITIL** – um conjunto complementar de publicações com orientações específicas para setores da indústria, tipos de organização, modelos operacionais e arquiteturas de tecnologia.

O Núcleo do ITIL, representado na figura a seguir, comprehende as fases de Estratégia do Serviço (*Service Strategy*), Desenho do Serviço (*Service Design*), Transição de Serviço (*Service Transition*), Operação de Serviço (*Service Operation*) e Melhoria de Serviço Continuada (*Continual Service Improvement*). Cada uma das fases do Núcleo do ITIL se tornou uma publicação dentro da biblioteca. Tais fases serão detalhadas nos tópicos 2.6.2 a 2.6.6. É importante dizer que outro componente básico da biblioteca, os “Guias Complementares”, são representados pelo anel cinza e divididos em publicações complementares, como livros, artigos, etc. e serviços de suporte web, como portais, *templates* etc.

Figura 2.7 – Núcleo do ITIL



Fonte: <http://www.itil.org>.

2.6.2 Estratégia do Serviço (Service Strategy)

É a fase na qual são fornecidas orientações úteis para o desenvolvimento de políticas e objetivos de gerenciamento do serviço por meio do seu ciclo de vida. Esta não é uma fase operacional, nesta fase são criadas políticas e decisões estratégicas acerca do funcionamento da TI. Os processos desta fase ajudam a organização na identificação do dono do serviço e dos donos dos processos, além de verificar a viabilidade e a importância da criação do serviço.

O ciclo de vida de estratégia contém cinco processos:

- ✖ Gerenciamento Estratégico para Serviços de TI;
- ✖ Gerenciamento de Portfolio de Serviço;
- ✖ Gerenciamento Financeiro para Serviços de TI;
- ✖ Gerenciamento de Relacionamento de Negócio;
- ✖ Gerenciamento de Demanda.

O **gerenciamento estratégico para serviços de TI** garante que existe um alinhamento estratégico entre a TI e o negócio, ou seja, a TI entende qual a estratégia do negócio e suporta esta estratégia. A estratégia de TI não deve ser simplesmente algumas palavras mortas, mas ser direcionada pelas ações e serviços disponibilizados pela organização.

Saiba mais

O alinhamento estratégico é o processo de transformar a estratégia do negócio em estratégias e ações de TI que garantem que os objetivos do negócio sejam apoiados.

Este processo define e mantém os 4 “Ps” da organização (perspectiva, posição, plano e padrões) no que concerne aos serviços de TI. O propósito é articular como um provedor de serviços irá possibilitar que uma organização alcance os seus resultados de negócio.

- ✖ **Estratégia de perspectiva:** é a visão da organização. Define seus valores e convicções. Determinará a direção na qual o provedor de serviço vai alcançar seus objetivos.

- × **Posição:** define qual é a imagem que a organização terá perante os clientes, tratando da definição de serviços que serão oferecidos para um mercado específico. Ela pode querer passar uma imagem de serviços com preço baixo e baixo valor agregado ou serviços de alto nível com preço elevado.
- × **Plano:** a estratégia é um plano de ação da organização para tornar-se competitiva. O plano descreve como ela vai executar a estratégia.
- × **Padrão:** representa os procedimentos da organização. Como resultado da perspectiva, posição e plano da estratégia surgem os padrões que guiam as atividades para executar a estratégia.

O **gerenciamento do portfólio** de serviço garante que os serviços em operação sejam escolhidos sob algum critério e estejam alinhados com a estratégia da TI. Um portfólio consistente garante que o departamento de TI saiba o que exatamente está fazendo e garante que os projetos executados irão agregar valor ao negócio.

Os tomadores de decisões da organização devem ser conscientizados que executar um projeto de TI demanda recursos – pessoas, aplicativos, infraestrutura – e como estes são limitados, a organização deve sempre escolher corretamente onde estes serão investidos. O correto gerenciamento de portfólio de serviços auxilia a organização a escolher em quais serviços os seus recursos serão utilizados.

O portfólio engloba desde os serviços que estão em fase de obsolescência até os serviços em análise de viabilidade. Os serviços do Portfólio devem ser descritos em termos do valor para o negócio, facilitando desta maneira as decisões de investimento. Seguem alguns questionamentos que devem ser abordados na descrição dos serviços.

- × Por que um cliente deve comprar este serviço?
- × Por que um cliente compraria este serviço conosco?
- × Qual o modelo de negócio (preço)?
- × Quais são as forças, fraquezas, prioridades e riscos?
- × Como deverá ser alocado os recursos?

Os serviços que entrarem em operação deverão adicionar valor ao negócio, não devendo entrar em operação somente porque é uma boa prática do mercado, ou por ser uma boa ideia.

O **gerenciamento de relacionamento de negócio** é o processo responsável pela manutenção de um relacionamento positivo com os clientes. O gerenciamento de relacionamento de negócio identifica necessidades do cliente e garante que o provedor de serviço seja capaz de atender a essas necessidades com um catálogo de serviços adequado. Este processo tem vínculos fortes com o gerenciamento de nível de serviço. Este gerenciamento é feito pelo gerente de relacionamento de negócio responsável por manter o relacionamento com um ou mais clientes. Este papel é frequentemente combinado com o papel do gerente de nível de serviço.

O **gerenciamento de demanda** é o processo responsável pelo entendimento, previsão e influência da demanda do cliente por serviços. O gerenciamento de demanda trabalha com o gerenciamento de capacidade para garantir que o provedor de serviço tenha capacidade suficiente para atender à demanda exigida. Em um nível estratégico, o gerenciamento de demanda pode envolver análise de padrões de atividade de negócio e perfis de usuário, enquanto, em nível tático pode envolver o uso de cobrança diferenciada para estimular clientes a usar os serviços de TI em horários menos ocupados ou exigir atividades em curto prazo para responder à demanda inesperada ou à falha de um item de configuração.

2.6.3 Desenho do Serviço (Service Design)

Esta fase projeta os serviços para que eles estejam alinhados com a estratégia do negócio, ou seja, que o serviço entregue o valor requisitado e atinja os objetivos traçados na fase anterior. Para isso, esta fase assegura que os serviços e processos sejam estabelecidas de maneira projetada e não simplesmente de acordo com as necessidades imediatas.

Atuar somente sobre as necessidades imediatas, sem organização e planejamento, fazendo que os processos ou serviços cresçam de maneira orgânica, não é uma boa prática, entretanto não é possível conhecer todos os seus nuances e necessidades antecipadamente. Deste modo, é boa prática criar o projeto de maneira iterativa e incremental, ou seja, com ondas de planejamento.

Um dos principais produtos desta fase é o *Service Design Package (SDP)* ou o pacote de desenho de serviço definindo todos os aspectos de um serviço de TI e seus requisitos em cada fase do seu ciclo de vida. Este pacote é produzido para cada novo serviço de TI, mudança importante ou obsolescência de serviço de TI.

O pacote detalha todos os aspectos do serviço e os requisitos juntamente com todos os estágios subsequentes do seu ciclo de vida. Ele alimenta os processos da fase de transição de serviço com informações necessárias para o seu desenvolvimento.

O SDP entre outros contém: os requisitos do serviço, os contatos dos parceiros de negócio, cliente e interessados, topologia do serviço, critério de aceitação do serviço, plano de transição, etc. Este pacote será alimentado com informações de vários processos desta fase de desenho de serviços.

Esta fase é constituída dos seguintes processos.

- × **Coordenação de desenho:** é o processo responsável pela coordenação de todas as atividades de desenho de serviço, seus processos e recursos.
- × **Gerenciamento de catálogo de serviço:** é um banco de dados ou documento estruturado com informações sobre todos os serviços de TI de produção, incluindo aqueles disponíveis para implantação.
- × **Gerenciamento do nível de serviços:** negocia os acordos acerca do funcionamento dos serviços com o negócio. Este processo gera o acordo do nível de serviços (ANS) ou *Service Level Agreement (SLA)*.
- × **Gerenciamento de segurança da informação (ISM):** todos os serviços devem ser implantados de maneira que respeitem as políticas de segurança de informação.
- × **Gerenciamento de fornecedor:** o propósito deste processo é garantir que os fornecedores entreguem serviços com a qualidade perfeita para o negócio, certificando-se de que o valor entregue seja custo-efetivo.

2.6.4 Transição do Serviço (Service Transition)

Este estágio tem como foco o gerenciamento das mudanças e novos serviços inseridos no ambiente da TI. A maioria dos incidentes e dificuldades que emergem no ambiente da TI são disparados por causa de problemas, por exemplo: a liberação de uma nova versão de um software poderá criar vários incidentes caso exista algum bug, a atualização do sistema operacional poderá criar vários incidentes caso o usuário não receba o correto treinamento. Entretanto, o avanço e novidades de mercado vem de mudanças, como novos serviços, atualizações e processos. Portanto neste estágio estão agrupados processos que asseguraram que as mudanças e a inserção de novos serviços sejam planejados e comunicados, minimizando os incidentes.

Os processos neste estágio são:

- ✖ **planejamento e suporte da transição** – é responsável por coordenar todas as atividades e recursos assegurando que os requisitos dos estágios de *Service Strategy* e *Service Design* serão efetivamente entregues no estágio de *Service Operation*.
- ✖ **gerenciamento de mudanças** – as mudanças são responsáveis por desencadear a maioria dos incidentes em um ambiente de TI, entretanto mudanças são responsáveis pela inovação do seu ambiente, portanto é necessário garantir que as mudanças implantadas sejam proveitosas ou necessárias para a organização.
- ✖ **gerenciamento de configurações e ativos de serviço** – o processo responsável por garantir que os ativos requeridos para entregar serviços sejam devidamente controlados e que informações precisas e confiáveis sobre esses ativos estejam disponíveis quando e onde forem necessárias.
- ✖ **gerenciamento de liberação e implantação** – neste processo será planejada, programada e controlada a construção, o teste e a implantação de liberações e, pela entrega de novas funcionalidades exigidas pelo negócio enquanto protege a integridade dos serviços existentes.
- ✖ **validação e teste do serviço** – é onde será feita a validação e teste de um serviço de TI novo ou modificado. A validação e teste de

serviço garante que o serviço de TI cumpre com sua especificação de desenho e que atenderá às necessidades do negócio.

- × **avaliação da mudança** – o processo responsável pela avaliação formal de um serviço de TI novo ou alterado para garantir que os riscos tenham sido gerenciados e para ajudar a determinar se a mudança deve ser autorizada.
- × **gerenciamento do conhecimento** – responsável por compartilhar perspectivas, ideias, experiência e informações, e por garantir que estejam disponíveis no lugar certo, no momento certo. Para a realização de maneira eficiente é necessário a utilização de um sistema de gerenciamento do conhecimento de serviço (SKMS).

2.6.5 Operação do Serviço (Service Operation)

Este estágio pode ser definido como o estágio cujo objetivo é garantir que os serviços de TI sejam entregues de forma eficaz e eficiente. A operação do serviço coordena e desempenha as atividades e os processos requeridos para entregar e gerenciar serviços em níveis acordados para usuários de negócio e clientes. É ineficiente quando um serviço alinhado com as estratégias da empresa, projetado e implantado corretamente, é operado de maneira desastrosa. Os outros estágios constroem um serviço para que a sua execução seja suave e benéfica para o usuário e para a empresa, mas é neste estágio que o valor do serviço é realmente entregue ao cliente.

Adicionalmente a operação de serviço gerencia a tecnologia que é usada para entregar e dar suporte a serviços, garantindo a correta operação de toda a infraestrutura de TI.

A operação de serviço inclui os seguintes processos.

- × Gerenciamento de evento;
- × Gerenciamento de incidente;
- × Cumprimento de requisição;
- × Gerenciamento de problema;
- × Gerenciamento de acesso.

E as seguintes funções.

- × Central de serviço;
- × Gerenciamento técnico;
- × Gerenciamento de operações de TI;
- × Gerenciamento de aplicativo.

2.6.6 Melhoria Continua de Serviço (Continual Service Improvement)

A Melhoria Contínua do Serviço (CSI – *Continual Service Improvement*) usa uma abordagem baseada em métricas para identificar oportunidades de melhoria e medir o impacto dos seus esforços. A CSI só pode ser eficaz se estiver integrado ao longo do ciclo de vida, criando uma cultura de melhoria contínua. Deve assegurar que todos os participantes na prestação de serviços compreendam que identificar as oportunidades de melhoria é também sua responsabilidade.

Neste contexto, uma tarefa importante é identificar quais métricas devem ser monitoradas. Isto é feito identificando, para cada serviço ou processo, quais são os fatores críticos de sucesso. Recomenda-se que cada processo ou serviço possua não mais que cinco fatores. Para determinar se os fatores críticos de sucesso estão presentes, é necessário identificar indicadores-chave de desempenho que representem o grau em que o fator está presente.

A Melhoria Contínua de Serviço usa um processo de sete etapas para orientar como os dados são coletados e utilizados.

1. Definir os objetivos;
2. Definição do que será mensurado;
3. Coletar os dados;
4. Processar os dados;
5. Analisar os dados;
6. Apresentar as informações;
7. Implementar melhorias.

Se a CSI estiver desempenhando corretamente seu papel, haverá sugestões de melhoria provenientes de todas as partes. É improvável que a organiza-

ção tenha recursos suficientes para implementar todas as sugestões, portanto é necessário visualizar as oportunidades de melhoria, entender seu impacto, escopo, requisitos de recursos e priorizar sua implementação.

Como as empresas possuem elevada dependência dos serviços de TI, é vital que as organizações avaliem e melhorem continuamente seus serviços de TI e os processos de gerenciamento que permitem esses serviços. É necessária uma prática contínua de melhoria contínua de serviço (CSI) formal para atender e alcançar os acordos de nível de serviço.

Síntese

Neste capítulo aprendemos as principais normas e padrões adotados mundialmente na atualidade relacionados à segurança da informação. É de fundamental importância que o profissional de TI conheça as normas ISO 27001, que tratam sobre a implementação de um SGSI (Sistema de Gestão de Segurança da Informação), bem como a ISO 27002, que é um documento de orientação para a efetiva implantação dos controles de segurança da informação comumente aceitos. Além das normas da família ISO, o COBIT apresenta-se como referência a uma organização que deseja ter uma governança de TI mais controlada. Por fim, nosso estudo com o ITIL apresentou um dos padrões mais utilizados para implantar o gerenciamento de serviços de TI em uma organização.

Atividades

1. Conceitue SGSI e explique qual a sua importância dentro de uma organização.
2. Um dos tópicos da NBR ISO/IEC 27002:2013 é a Segurança Física e do Ambiente. Exemplifique um caso em que a falha neste aspecto possa causar um incidente de segurança em uma organização.
3. Cite os cinco princípios básicos do COBIT v.5, que norteiam a governança e gestão de TI de uma organização.
4. Conceitue os dois componentes básicos do ITIL, fornecendo uma descrição resumida para cada um destes.

3

Procedimentos e Boas Práticas de Segurança da Informação

No CAPÍTULO ANTERIOR estudamos as normas relacionadas à segurança da informação. Pretendemos neste capítulo abordar as melhores práticas e procedimentos relacionados à aplicação destas normas, para que o profissional gestor de Tecnologia da Informação tenha condições de aplicar na prática o que as normas recomendam.

ABORDAREMOS QUESTÓES RELACIONADAS à utilização dos recursos de TI por parte dos funcionários de uma organização, bem como aspectos relacionados à segurança física (em especial *data-center*) e à segurança lógica. Também abordaremos metodologias que visam minimizar os problemas que os administradores de rede encontram para implementar segurança na rede de dados. Assuntos importantes como política de senhas e políticas de backup também serão abordados neste capítulo.

Objetivo de aprendizagem:

- × Promover a capacitação para a adoção de práticas de segurança da informação no ambiente corporativo.

3.1 Utilização dos recursos de TI

É de fundamental importância que a organização possua uma política de utilização dos recursos de TI bem definida. É sabido que a maioria dos incidentes de segurança da informação ocorrem no ambiente interno das organizações, sendo que a maior fatia de recursos financeiros normalmente é investida no ambiente externo, com altos custos de aquisição de itens como: *firewall*, IDS, IPS, entre outros (conceitos serão abordados nos tópicos a seguir). Se as equipes internas das organizações não forem bem instruídas isto pode se tornar um grande problema.

Os colaboradores da instituição devem ter ciência de que o uso dos recursos tecnológicos deve ser feito apenas para atividades diretamente relacionadas aos negócios da organização. Devem ser instruídos a respeito da não-proliferação de conteúdo discriminatório em razão de sexo, raça, religião, condição de saúde ou qualquer outra condição pertinente. Devem também estar cientes de que não podem usar os recursos tecnológicos para fins de obtenção, cópia e distribuição de material protegido por direito autoral.

Cabe à equipe de TI disponibilizar aos colaboradores (funcionários ou terceiros) somente os recursos tecnológicos que irão auxiliá-los no desempenho de suas funções e execução de seus trabalhos. A equipe deve efetuar a instalação de programas necessários para o desenvolvimento de suas atividades, bem como avaliar a liberação de instalação de outros programas que não sejam diretamente ligados ao desempenho das funções. Outro exemplo de boa prática a ser implementada pelo administrador de TI é o bloqueio da instalação direta de *softwares* por parte do usuário final. Tais instalações devem ser realizadas apenas com credenciais administrativas de domínio, de posse da equipe de suporte de TI.

Saiba mais

Você pode consultar um exemplo de regulamento de gestão e utilização de recursos de tecnologia da informação em uma instituição governamental neste endereço da internet: <<http://www.tce.pe.gov.br/internet/docs/resolucoes/14res0017.pdf>>.

3.2 Titularidade das informações

Monitoramento é um assunto delicado e muitas vezes polêmico no mundo corporativo. Apesar de existir uma ampla proteção jurídica ao cidadão a respeito da violação indevida de sua privacidade, é importante instruir os colaboradores de que, dentro do ambiente corporativo, a empresa detém os direitos sobre todos os dados e informações armazenados nos seus ambientes computacionais. Mensagens, dados e informações enviadas e recebidas em sistemas de correio eletrônico e correio de voz também estão sujeitas a monitoramento. É importante que o funcionário ou terceiro não utilize o e-mail corporativo de maneira indevida, negligente ou maliciosa, pois pode haver consequências e responsabilidades para a empresa.

A equipe de TI deve estar respaldada, por meio da política de segurança da informação da empresa, para efetuar o acesso e monitoramento de todos os meios tecnológicos, incluindo computadores, sistemas de correio eletrônico, internet, correio de voz etc.

Quanto ao sistema de correio eletrônico, embora possa haver questionamento jurídico a respeito do tema, a maioria dos tribunais e decisões judiciais tem sido no sentido de que se o empregado for previamente avisado que o e-mail da empresa deve ser usado apenas para fins profissionais, a empresa poderá monitorar o conteúdo sem ferir a norma constitucional. No entanto, se o empregado eventualmente utilizar o e-mail corporativo para assuntos particulares, deve ter consciência de que o acesso pela empresa ou pelo empregador não caracteriza violação de sua privacidade ou intimidade.

3.3 Perímetro de segurança

Estudamos no capítulo anterior as principais normas de segurança da informação da família 27000. Uma das medidas contida nestas normas trata das barreiras de segurança, que são quaisquer medidas com o objetivo de prevenir ataques aos ativos da informação. Tais medidas constituem-se de barreiras físicas, como fechaduras magnéticas e muros, ou lógicas, por exemplo um mecanismo de senha.

Lyra (2008) define perímetro de segurança como “o contorno ou linha imaginária que delimita uma área ou região separada de outros espaços físicos por um conjunto qualquer de barreiras”.

É importante estabelecer de forma clara qual é o perímetro de segurança, pois assim ficará mais fácil definir onde serão investidos mais recursos para a proteção do ativo de informação.

3.4 Segurança no ambiente físico

Outro aspecto importante é a garantia da segurança no ambiente físico. Deve ser elaborado um projeto de áreas de segurança que conteplane um perímetro seguro, como um escritório fechado ou com várias salas, onde sejam consideradas ameaças como fogo, poeira, explosão ou desastres naturais. É importante também que haja um treinamento específico para profissionais que prestam serviços como limpeza e manutenção.

Qualquer acesso às dependências de uma organização deve ser controlado, sempre efetuando a necessária formalização. Uma das formas de garantir isto é que seja implementado uma metodologia de acesso na qual somente profissionais autorizados possam ingressar em um setor. Além disso, todos os funcionários da instituição devem portar identificação funcional visível. Para áreas mais restritas os acessos devem ser previamente solicitados e autorizados, por meio de procedimentos formais criados para tal atividade.

Em relação a terceiros, como prestadores de serviços (contratados para consultorias, contratados para manutenções, entre outros), deverão obter autorização formal antecipada para acesso às dependências.

De acordo com a norma NBR 11514 (controle de acesso para segurança física de instalações de processamento de dados), as áreas consideradas de risco elevado, ou seja, quando há risco de comprometimento de continuidade de negócios, devem possuir procedimentos de forma que seja possível monitorar, por meio de câmeras de vigilância, o *hall* de entrada e as áreas críticas da organização.

3.4.1 Segurança em datacenter

Não é novidade que o *datacenter* (centro de processamento de dados) é considerado o local mais adequado para processamento e armazenamento de dados corporativos de forma segura. Porém, ainda é um desafio grande para muitas empresas manter este ambiente totalmente seguro. Para que isso aconteça, é de fundamental importância que pontos falhos sejam eliminados.

Sabemos que não existe um ambiente totalmente imune a falhas ou à desastres. Mas, por outro lado, é possível prevenir-se ao detectar as ameaças com a antecedência necessária para tomar providências que impeçam impactos no ambiente de trabalho. Para isso, é necessário conhecer e diagnosticar os riscos que um *datacenter* pode sofrer.

A figura 3.1 exemplifica quatro requisitos de segurança básicos que um *datacenter* precisa possuir.

Figura 3.1 – Requisitos de segurança em *datacenter*



Fonte: Elaborada com elementos de Shutterstock.com/nasirkhan.

- × **Controle de acesso:** é indispensável que a organização crie políticas de acesso rigorosas para controle de quais pessoas podem ou não entrar no ambiente do *datacenter*. Esta segurança poderá ser feita de diversas formas, como: biometria, crachá com sensor de presença, código de acesso individual (senha), entre outros.
- × **Proteção contra danos:** o *datacenter* armazena todos dados e informações críticas de uma organização e qualquer dano físico pode comprometer a continuidade dos negócios, acarretando prejuízos financeiros significativos. Portanto, é necessário que o *datacenter* esteja protegido contra quaisquer riscos físicos que possam causar danos e interromper as atividades da empresa, tais como: incêndios, sobrecarga elétrica, vazamentos e desastres naturais.
- × **Manutenção periódica:** para diminuir de forma significativa o risco de falhas inesperadas na operação, é imperioso que o *datacenter* passe por manutenções preventivas, adaptações e trocas de equipamentos, em intervalos de tempo regulares e não muito espaçados. Dessa forma, é possível garantir a segurança das operações do *datacenter* a longo prazo.
- × **Refrigeração do ambiente:** assim como grande parte dos equipamentos eletrônicos, os equipamentos de um *datacenter* produzem calor e, caso não estejam recebendo a refrigeração indicada por seus fabricantes, os riscos de uma parada nas operações ou até de um incêndio passam a ser maiores. É importante contar com sistemas de monitoramento de temperatura, que indiquem qualquer discrepância pois, dessa forma, os técnicos de manutenção podem agir em tempo hábil. Não se pode deixar de contar também com sistemas redundantes, pois em caso de falha de um equipamento, outro assume a tarefa de manter o ambiente refrigerado.

3.5 Segurança de documentos em papel e documentos eletrônicos

Ao mesmo tempo em que as organizações necessitam efetuar a guarda de documentos de valor por um longo prazo, também devem levar em conta

que são necessários mecanismos de proteção compatíveis com o meio em que o documento foi produzido.

Para a proteção adequada dos documentos em papel é necessário a adoção de procedimentos de tratamento de cópias, armazenamento, transmissão e descarte seguros. Os documentos em papel exigem cuidados como armazenar em ambiente adequado, a fim de evitar problemas com umidade, entre outros. É recomendável a utilização de rótulos para identificação dos documentos e manter procedimentos especiais para impressão, cópia e transmissão, bem como para recepção e envio de correspondências sigilosas. Existem papéis que são mais sensíveis à ação do tempo e luz solar, como papéis térmicos por exemplo.

Documentos eletrônicos, por sua vez, trazem outras questões relacionadas ao seu armazenamento. Além dos aspectos da tríade CID (confidencialidade, integridade e disponibilidade) que devem ser observados, deve ser adicionada também a questão da obsolescência tecnológica. Vide o caso de disquetes, que já não podem mais ser lidos pela maioria dos equipamentos modernos.

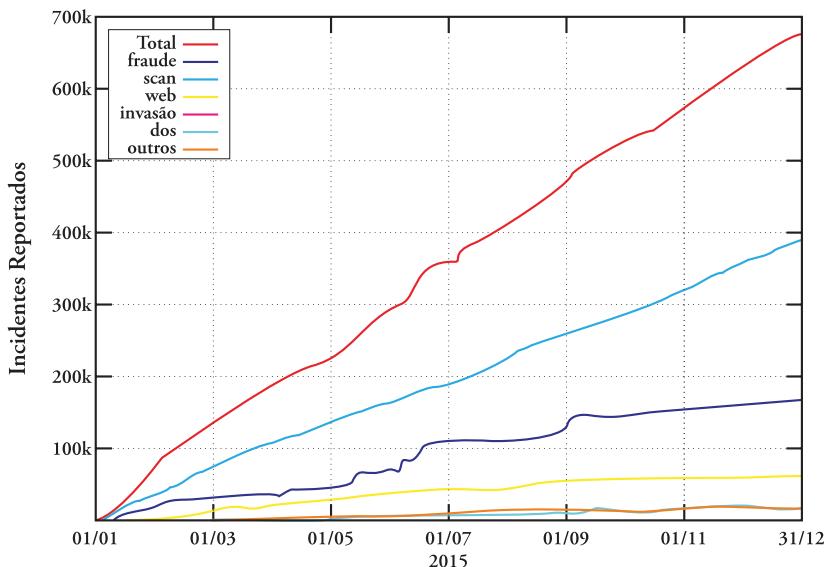
3.6 Segurança no ambiente lógico

Iniciaremos o nosso estudo sobre segurança no ambiente lógico falando sobre Segurança em Redes. A segurança em redes se refere a estratégia e provisões de uma organização para garantir a segurança de seus ativos de informação durante todo o tráfego de rede. As preocupações com a segurança das redes devem abranger as situações que envolvam autenticação dos usuários aos serviços autorizados, contemplando o estabelecimento de interfaces seguras entre a rede interna e a rede pública ou de outra organização (LYRA, 2008).

À medida que houve um incremento ao longo do tempo quanto ao número de equipamentos interconectados em redes, aumentou também significativamente as tentativas de ataque, bem como as invasões bem-sucedidas destes equipamentos.

Para percebermos a dimensão que este problema representa aos administradores de redes, vamos visualizar as estatísticas de incidentes reportados em 2015, classificados por tipos de ataques acumulados, indicados na figura a seguir.

Figura 3.2 – Incidentes reportados ao CERT.br (tipos de ataques acumulados)



Obs.: este gráfico não inclui os dados referentes a worms.

DoS (Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

Invasão: um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede.

web: um caso particular de ataque visando especificamente o comprometimento de servidores web ou desconfigurações de páginas na internet.

Scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Fraude: segundo Houaiss (2016), é “qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever;

logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

Outros: notificações de incidentes que não se enquadram nas categorias anteriores.

Fonte: CERT.br (2016).

3.6.1 Arquitetura TCP/IP e suas fragilidades

No início dos anos 1980 foram finalizadas as especificações para os protocolos TCP e IP. Estes dois protocolos podem ser considerados os mais importantes atualmente, pois são a base do funcionamento da internet. Ao longo das últimas décadas, a internet cresceu de uma pequena rede conectando uma pequena comunidade de pesquisadores até o seu estágio atual: uma gigantesca rede global conectando pessoas de todos os lugares do planeta.

O enorme sucesso da internet tem sido, em sua maioria, bastante benéfico. A internet evoluiu de um projeto especializado para uma ferramenta de propósito geral. No entanto, seu crescimento criou problemas no que se refere a segurança. Os protocolos TCP e IP foram concebidos quando ela era pequena e os utilizadores normalmente confiavam uns nos outros. Estes protocolos carecem de muitos recursos que são desejáveis ou necessários em uma rede insegura, como por exemplo recursos de autenticação ou criptografia.

À medida que a utilização dos protocolos TCP/IP aumenta, a falta de segurança incorporada torna-se cada vez mais problemática. Com o advento de novas ferramentas e técnicas que possibilitam ataques às redes, as fragilidades dos protocolos TCP/IP passaram a ser exploradas com mais frequência. A seguir, exemplificamos alguns destes ataques que podem ser praticados utilizando-se destas vulnerabilidades.

- ✖ **IP spoofing:** é técnica para criação de pacotes do protocolo IP com um endereço falso de origem, com a finalidade de mascarar (*spoof*) a identidade do remetente.
- ✖ **DoS:** sigla para *Denial of Service*, que literalmente significa “negação de serviços”. Este ataque consiste em tentativas de fazer com que computadores, em especial servidores web, tenham dificuldade ou mesmo sejam impedidos de executar suas tarefas. Para tal,

ao invés de tentar invadir um servidor, ou mesmo infectá-lo com algum tipo de *malware*, o autor do ataque faz com que a máquina receba tantas requisições que esta chega ao ponto de não conseguir responder a todas elas. Resumidamente, o computador fica tão sobrecarregado que nega o serviço.

- ✖ **DDoS:** é a sigla para *Distributed Denial of Service*, que literalmente significa “negação de serviços distribuída”. É um tipo de ataque DoS de grandes proporções, ou seja, que utiliza até milhares de computadores para atacar um determinado servidor, distribuindo a ação entre todas as máquinas participantes do ataque. Trata-se de uma forma que aparece constantemente em noticiários, pois é o tipo de ataque mais comum na internet. Normalmente utiliza-se das chamadas “redes zumbis”, que são máquinas infectadas por *malwares* que respondem remotamente à ordem de quem está coordenando os ataques. Muitos computadores fazem partes destas redes sem que os seus proprietários tenham conhecimento do fato.
- ✖ **Trojan Horses:** este termo significa “cavalo de Tróia”. É um tipo de programa malicioso que pode entrar em um computador disfarçado como um programa comum e legítimo. Ele serve para possibilitar a abertura de uma porta de entrada, de forma que usuários mal-intencionados possam invadir um sistema computacional.
- ✖ **TCP Hijacking:** este ataque é conhecido como “roubo de sessão TCP” ou “sequestro de sessão”. Trata-se de um método de maior complexidade, que visa assumir uma sessão entre duas máquinas em rede, obtendo o ID de sessão e disfarçando-se como um usuário autorizado. Uma vez que o ID de sessão do usuário tenha sido adquirido (por meio da previsão de sessão), o invasor pode mascarar-se como sendo o usuário original e fazer qualquer coisa que o mesmo esteja autorizado a fazer na rede. A intrusão pode ou não ser detectável, dependendo do nível de conhecimento técnico do usuário e da natureza do ataque. Por exemplo, se um site da web não responde da maneira normal ou esperada ou, para de responder completamente por uma razão desconhecida, o sequestro de sessão pode ser uma possível causa.

- ✖ **Sniffing:** é uma técnica que possibilita interceptar e registrar o tráfego de rede entre dois ou mais computadores. Utiliza-se de uma ferramenta (*sniffer*) que faz a captura de cada pacote, podendo o mesmo ser decodificado e tendo seu conteúdo exposto. Embora possa ser utilizada para fins benéficos, como análise de tráfego de rede, um invasor pode obter uma cópia do arquivo, ou até mesmo senhas utilizando-se desta técnica.

Saiba mais

A nova versão do protocolo IP, o IPv6, trouxe uma série de melhorias, sendo uma das principais a preocupação de corrigir as limitações de segurança existentes no IPv4. Um dos principais mecanismos criados para isso é o *IPSec (IP Security)*, que fornece funcionalidades de criptografia de pacotes de dados, de forma a garantir integridade, confidencialidade e autenticidade.

Importante

A criptografia caracteriza-se como uma das funcionalidades mais elementares na proteção de uma rede de dados. Abordaremos este tema de maneira mais ampla no próximo capítulo.

3.6.2 Firewalls

Os *firewalls* são dispositivos de segurança de rede que concedem ou rejeitam o acesso de rede a fluxos de tráfego entre uma zona não confiável (por exemplo, a internet) e uma zona confiável (por exemplo, uma rede privada ou corporativa). Os dispositivos de *firewall* são um conjunto de ferramentas instaladas e configuradas para trabalhar em conjunto em um determinado equipamento.

Quando as organizações começaram a passar de computadores *mainframe* e clientes isolados para o modelo cliente-servidor, a capacidade de con-

trolar o acesso ao servidor tornou-se uma prioridade. Antes que os *firewalls* surgissem no final da década de 1980, a única forma real de segurança da rede era realizada por listas de controle de acesso (ACLs) residentes em roteadores. As ACLs determinavam a quais endereços IP era concedido ou negado o acesso à rede.

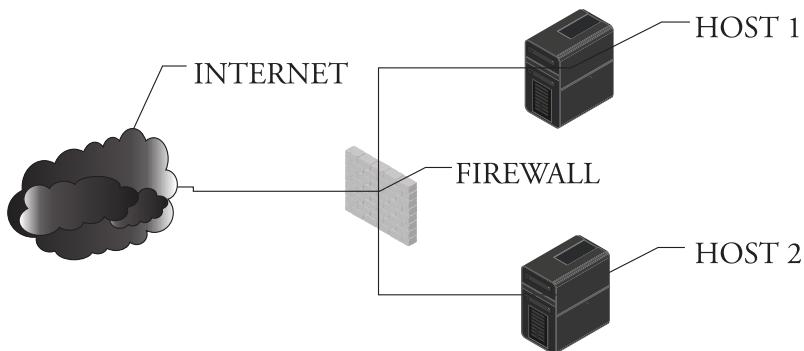
O crescimento da internet e o resultante aumento da conectividade das redes evidenciou que este tipo de filtragem já não era suficiente para impedir o tráfego malicioso, uma vez que apenas as informações básicas sobre o tráfego de rede estão contidas nos cabeçalhos dos pacotes. A tecnologia de *firewall* evoluiu desde então para combater a crescente sofisticação dos ataques cibernéticos.

Um *firewall* pode ser baseado em *hardware* ou *software*, sendo que este último é mais comum. A expressão “parede de fogo” (tradução literal de *firewall*) deixa claro que o *firewall* se enquadra em uma espécie de barreira de defesa, bloqueando tráfego de dados indesejado e liberando acessos que não representam risco.

Um *firewall*, isoladamente, não é capaz de proteger totalmente uma rede ou um computador. Assim como um edifício necessita de vários itens de segurança (muros, portões, câmeras de vigilância, alarmes) que fazem a segurança de maneira conjunta, o *firewall* também deve ser utilizado em conjunto com outros recursos, como antivírus, IDS, VPN etc. Desta forma, quando somente um destes itens está sendo utilizado, há menor eficiência de proteção.

Uma das arquiteturas mais simples e utilizadas para implementação de *firewall* é a “*Dual-Homed Host*”, exemplificada na figura 3.3. Consiste de equipamento que intercala e divide duas redes de forma centralizada. Este equipamento é composto por duas placas de redes e age como roteador, interligando as redes. A principal vantagem desta abordagem é que há grande controle do tráfego. A desvantagem mais expressiva, no entanto, é que qualquer problema com o equipamento que suporta o *firewall* pode pôr em risco a segurança da rede ou mesmo paralisar o tráfego. Por este motivo, o seu uso pode não ser adequado em redes cujo acesso à internet é essencial.

Figura 3.3 – Ilustração de um *firewall* na arquitetura *dual-homed host*



Fonte: Elaborada com elementos de Shutterstock.com/Grimgram.

Saiba mais

Além da arquitetura *dual-homed host*, existem também a *screened host* e a *screened subnet*, cujas implementações, embora mais complexas, apresentam resultados mais satisfatórios em ambientes corporativos de maior porte.

3.6.3 Sistema de detecção de intrusão (IDS)

O IDS, sigla para *Intrusion Detection System*, significa sistema de detecção de intrusão. O modelo de detecção de intrusão baseia-se na premissa de que o padrão de comportamento de um agente intruso é diferente o bastante de um usuário legítimo, de forma que possa ser detectado por análises de estatísticas de uso.

Desta forma o IDS é um mecanismo capaz de identificar ou detectar a presença de atividades intrusivas, englobando todos os processos utilizados na descoberta de utilizações não autorizadas de dispositivos de rede ou de computadores.

A implementação de uma ferramenta de IDS é fundamental em uma arquitetura de segurança de redes pois este recurso é capaz de manter a infra-estrutura distante de ataques indesejados.

3.6.4 Sistema de prevenção de intrusão (IPS)

O IPS, sigla para *Intrusion Prevention System*, caracteriza-se por ser uma evolução do IDS. O IDS apenas efetua o monitoramento e registro em *logs* das atividades suspeitas em uma rede, permitindo que o administrador decida como parar o ataque. Já o IPS pode ser configurado para que, ao perceber uma tentativa de invasão, uma ação seja tomada automaticamente. Estas ações incluem gerar uma alerta, bloquear o atacante, bloquear os pacotes que trafegam, entre outras.

Saiba mais

Existem também os sistemas mistos, denominados Sistemas de Detecção e Prevenção de Intrusão (*Intrusion Detection and Prevention System – IDPS*), que surgiram a partir da união dos sistemas IDS e IPS. Administradores de rede tem a opção de desativar as funções de IPS, fazendo com que o sistema passe a funcionar apenas como IDS.

3.6.5 Redes de perímetro (DMZ)

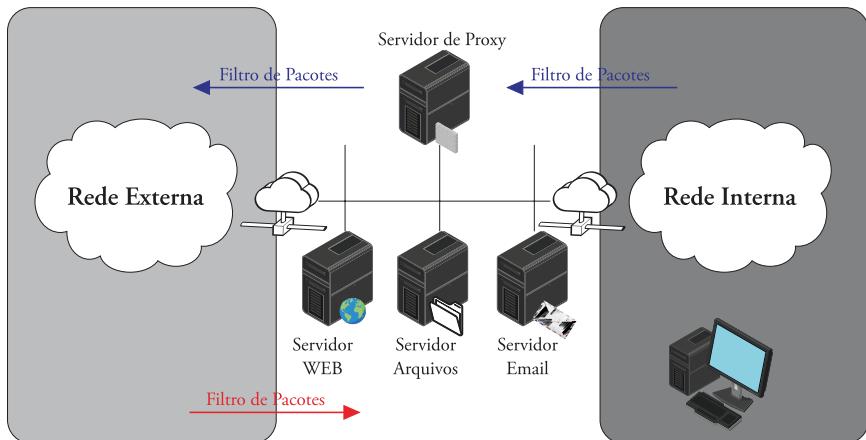
As denominadas redes de perímetro ou zona desmilitarizada (DMZ – *Demilitarized Zone*), permitem proteger um computador ou conjunto destes, posicionando-se entre uma rede interna e a internet. O termo vem do uso militar, significando uma área neutra que separa dois inimigos. Trata-se de um conceito de implementação e configuração, não sendo um *hardware* ou *software* específico que efetua esta função.

Sua função é manter os serviços que possuem acesso externo separados da rede local, restringindo ao máximo um potencial dano causado por algum invasor, tanto interno como externo.

A DMZ permite o acesso de usuários externos aos servidores específicos localizados na rede de perímetro, ao mesmo tempo em que evita o acesso à

rede corporativa interna. A figura a seguir ilustra a implementação de uma DMZ em uma corporação que possui servidores ou serviços sendo acessados por público externo:

Figura 3.4 – Exemplo de rede de perímetro (DMZ)



Fonte: Reproduzido de <http://www.diegomacedo.com.br> com elementos de Shutterstock.com/Grimgram/FTillaev/peiyang.

3.6.6 Virtual Private Network (VPN)

O conceito de rede privada virtual (*Virtual Private Network* – VPN) surgiu da necessidade de utilizar redes de comunicação públicas (não confiáveis) para trafegar informações privadas de forma segura. Tendo em vista que os dados que trafegam em uma rede pública estão sujeitos a interceptação e captura, a VPN é uma opção de custo relativamente baixo para organizações que necessitem interligar suas operações.

Uma das grandes vantagens encontradas no uso de VPN é a diminuição de custos com comunicações corporativas, pois elimina a necessidade de links dedicados de longa distância que podem ser substituídos pela internet. As redes corporativas podem, por meio de links dedicados, conectar-se a algum provedor de acesso local e interligar-se a outras redes corporativas, possibilitando o fluxo de dados seguro por meio da internet. Esta solução torna-se bastante viável sob o ponto de vista financeiro, sobretudo nos casos em que

enlaces internacionais ou nacionais de longa distância estão envolvidos, o que representaria um alto custo de implementação para uma rede privativa.

A implementação de solução de VPN em empresas deve ser acompanhada de estudos e planejamento, visto que as transmissões de dados por essas redes normalmente são mais lentas e necessitam de uma conexão à internet razoavelmente rápida.

3.7 Política para acesso à internet

O objetivo principal de criar uma política de acesso à internet para as organizações é proteger a mesma contra a maioria das formas comuns de ameaças na internet.

Embora a conexão direta e permanente com a internet ofereça uma série de benefícios e potenciais de negócios para uma organização, deve-se ter em mente que também oferece riscos significativos para as informações da empresa se não houver uma rígida disciplina de segurança.

Enquanto um administrador de redes possui conhecimento suficiente para diferenciar conteúdo nocivo na internet, os colaboradores em geral não são tão conscientes da necessidade de uma navegação segura. Além disso, o crescimento das redes sociais é motivo de preocupação para muitos gestores, pois esses sites podem ser motivo de grande distração e decremento de produtividade.

Todas as conexões devem ser registradas por meio de sistemas de *logs*, para fins de auditoria. Minimamente devem conter os seguintes registros:

- a) identidade do usuário;
- b) data, hora e tempo de permanência das conexões;
- c) endereços IP e URL's acessadas (bloqueadas ou liberadas);
- d) protocolos utilizados;
- e) quantidade de dados enviados/recebidos.

Não há modelo padrão para uma política de segurança de internet e a maioria das empresas possuem sua própria política. O que será incluído depende do que os gestores entendem como uso aceitável e como seus funcio-

nários devem se comportar. No entanto, existem algumas premissas básicas que a política deve conter, e estas incluem (FERREIRA, 2008):

- a) se os funcionários terão permissão para navegar na web para uso pessoal, assim como para fins comerciais;
- b) se os funcionários poderão usar a internet para fins particulares, e em caso afirmativo, em quais períodos e por quanto tempo (durante o almoço, após o expediente etc.);
- c) se e como a organização efetuará o monitoramento do uso da internet e qual nível de privacidade os funcionários estarão sujeitos;
- d) acessos não permitidos, determinando os tipos de sites que serão inaceitáveis, como: download de conteúdo ofensivo ou preconceituoso, atitudes ameaçadoras ou violentas, atividades ilegais, solicitações comerciais (não relacionadas ao trabalho), e quaisquer outros aspectos que a organização julgar necessários.

Um dos erros comuns que muitas empresas cometem na produção de uma política de segurança para acesso à internet é fazer com que a política tenha dezenas de páginas, e com muitos termos legais e técnicos, transformando-a em uma longa lista de ameaças. A política, portanto, deve ter o objetivo principal de auxiliar os funcionários da instituição a entender as ameaças que o negócio enfrenta, caso ocorra um incidente de segurança.

Por último, será necessário verificar periodicamente a política para certificar-se de que ela está mantendo-se atualizada com as últimas inovações e tecnologias da internet.

3.8 Política para uso de correio eletrônico

O correio eletrônico é um meio muito eficiente para a troca de informações, porém existem diversas armadilhas que os colaboradores necessitam estar atentos, pois há o risco de disseminação de *malwares* pela rede local e internet.

Uma política de uso de correio eletrônico define as responsabilidades dos seus funcionários ao usar o e-mail em suas atividades diárias de trabalho.

O uso de correio eletrônico por funcionários de uma determinada organização deve ser permitido e incentivado quando tal uso apoia as metas e objetivos do negócio. No entanto, a organização deve ter uma política para o uso de e-mail pela qual o funcionário esteja ciente de alguns aspectos básicos, como: estar em conformidade com a legislação vigente, usar o e-mail de forma responsável e não criar riscos desnecessários para a empresa pelo mau uso desta ferramenta.

Elencamos a seguir alguns comportamentos considerados inaceitáveis em relação ao uso de correio eletrônico por parte de funcionários de uma organização.

- a) Uso de sistemas de comunicação da empresa para cuidar de negócios pessoais ou envio de “correntes”;
- b) Encaminhamento de mensagens confidenciais da empresa para locais externos;
- c) Distribuir ou armazenar imagens, textos ou materiais que possam ser considerados indecentes, pornográficos, obscenos ou ilegais;
- d) Distribuir ou armazenar imagens, textos ou materiais que possam ser considerados discriminatórios, ofensivos ou abusivos, com conteúdo sexista ou racista;
- e) Disseminação de materiais protegidos por direitos autorais;
- f) Invasão do sistema da empresa ou de outra organização através do uso não autorizado de uma senha de outrem;
- g) Difundir opiniões pessoais não solicitadas sobre questões sociais, políticas, religiosas ou outras questões não relacionadas com o negócio;
- h) Transmissão de material comercial ou publicitário não solicitado;
- i) Atividades deliberadas que desperdicem esforços pessoais ou recursos de rede;
- j) Introdução de qualquer forma de vírus de computador ou *malware* na rede corporativa, através da abertura de *links* considerados suspeitos;

É importante ressaltar que não constitui crime a monitoração do conteúdo de e-mails enviados ou recebidos pelos colaboradores de uma empresa,

para fins de auditoria e/ou investigação. É importante deixar isto claro em uma política de uso de correio eletrônico corporativo. Os recursos de e-mail de uma empresa são fornecidos para fins comerciais, portanto, a empresa mantém o direito de examinar quaisquer sistemas e inspecionar quaisquer dados registrados nesses sistemas.

Quando houver o descumprimento explícito de uma política de uso responsável de correio eletrônico por parte de um colaborador da empresa, a mesma poderá aplicar uma penalidade disciplinar que vai desde uma advertência verbal até demissão por justa causa. Os funcionários de uma determinada organização, contratados ou terceirizados que tenham obtido o direito de usar os serviços de e-mail desta deverão assinar um termo confirmado sua compreensão e aceitação da política.

3.9 Gerenciamento de logs

Nos séculos 18 e 19, as fortalezas militares colocavam sentinelas nos muros para manter vigilância constante na área circunvizinha. Se acontecesse alguma atividade suspeita, eles tocariam sinos, trombetas, ou gritariam para os companheiros do forte para alertá-los sobre o perigo iminente.

Atualmente as empresas possuem uma espécie de “sentinela eletrônica” na maioria dos seus sistemas denominados registros de *log*. Os sistemas de monitoramento supervisionam as atividades da rede, inspecionam eventos do sistema e armazenam ações do usuário (por exemplo, a ação de renomear um arquivo, abrir um aplicativo) que ocorrem dentro do sistema operacional. Eles são os vigias dos administradores e têm a capacidade de fornecer os dados que podem alertá-los sobre um incidente de segurança. Os arquivos de *log* brutos também são conhecidos como registros de auditoria, trilhas de auditoria ou *logs* de eventos.

A maioria dos sistemas e softwares geram *logs*, incluindo sistemas operacionais, navegadores de internet, estações de trabalho, *antimalwares*, *firewalls* e sistemas de detecção de intrusão (IDS). Mas vale salientar que alguns sistemas com capacidades de registrar *logs* não ativam automaticamente esta funcionalidade, portanto é importante garantir que todos os sistemas tenham esta funcionalidade ativada. Além disso, alguns sistemas geram *logs* mas não

fornecem soluções de gerenciamento destes *logs* de eventos. O administrador precisa estar ciente de seus recursos de sistemas e efetuar a instalação de *software* de monitoramento e gerenciamento de *logs*, quando necessário.

As análises de registros de *logs* podem mostrar atividades suspeitas do sistema. As empresas devem revisar seus registros diariamente (preferencialmente) para procurar erros, anomalias ou atividades suspeitas que se desviam da rotina da mesma.

Do ponto de vista da segurança, o objetivo de um *log* é agir como uma “bandeira vermelha”, alertando quando algo ruim está acontecendo. A análise regular de *logs* pode ajudar a identificar ataques maliciosos em um sistema de informações.

Dada a grande quantidade de dados de *log* gerados pelos sistemas, é impraticável rever diariamente todos esses *logs* manualmente. Existem *softwares* de monitoramento e análise de registros que cuidam dessa tarefa usando regras para automatizar a revisão desses *logs* e apenas apontar eventos que possam representar problemas ou ameaças. Muitas vezes isso é feito usando sistemas de relatórios em tempo real que alertam o administrador por e-mail ou mensagem de texto (SMS) quando algo suspeito é detectado.

Nem todos os sistemas de rede são exatamente os mesmos, e configurar as regras que irão filtrar a quantidade geralmente grande de *logs* gerados é muito importante e muitas vezes leva algum tempo até o administrador conseguir deixar tudo em ordem.

A seguir elegemos alguns tipos de eventos, que são de fundamental importância que sejam considerados por um administrador de serviços de TI, ao configurar seu sistema de gerenciamento de registros de *logs*.

- a) Alterações de senha;
- b) *Logins* não autorizados;
- c) Falhas de *login*;
- d) Novos eventos de *login*;
- e) Detecção de *malware*;
- f) Ataques de *malware* vistos pelo IDS;
- g) Escaneamento do *firewall* em busca de portas abertas;

- h) Ataques de negação de serviço (DoS / DDoS);
- i) Erros em dispositivos de rede;
- j) Alterações de nome de arquivos;
- k) Alterações na integridade dos arquivos;
- l) Dados exportados;
- m) Novos processos iniciados ou processos em execução parados;
- n) Eventos de compartilhamentos de rede;
- o) Eventos de conexão / desconexão remota;
- p) Nova instalação de serviços;
- q) Auditoria de arquivos;
- r) Novas contas de usuário;
- s) Valores de Registro modificados, entre outros.

É necessário também estabelecer uma rotina de proteção para os registros de *logs* armazenados, a fim de certificar-se de que os mesmos não foram maliciosamente alterados por criminosos cibernéticos ou accidentalmente alterados por funcionários bem-intencionados.

Uma organização deve atribuir um funcionário de confiança específico para a tarefa de revisar os principais *logs* diariamente. Deve também ter uma equipe de pessoas prontas para revisar alertas suspeitos. Boas práticas afirmam a necessidade de armazenamento dos registros por pelo menos 1 ano.

Importante

O maior problema com *logs* é: ninguém fica de olho neles!



3.10 Política de senhas

A política de senhas fortes tem percorrido um longo caminho desde a era da popularização dos computadores. As senhas são parte permanente da vida cotidiana de todos nós, à medida que mais e mais serviços que

utilizamos são gerenciados de forma *on-line* através de sites e aplicativos de dispositivos móveis.

Os usuários hoje são inundados com uma grande quantidade de senhas que devem se lembrar: senhas de sítios diversos na internet, contas de e-mail, contas em redes sociais, serviços bancários, sistemas de segurança doméstico, entre tantos outros serviços.

Criar uma política de senha forte é a chave para ajudar os usuários a proteger esses sistemas críticos, dos quais todos dependem diariamente. Embora a complexidade adicional possa parecer um inconveniente para muitos usuários, não deve impedir que uma política de senha forte seja implementada em sua organização.

As violações de segurança podem afetar organizações de diversas áreas e tamanhos. Desde pequenas até grandes corporações já tiveram sistemas comprometidos, expondo senhas de usuários. Alterar uma senha em um destes sites comprometidos nem sempre é suficiente. E as chances de que as senhas comprometidas sejam usadas em outros lugares, deixando os usuários vulneráveis aos *hackers* são altas, visto que muitos usuários possuem a mesma senha para diferentes serviços.

Anualmente é divulgado na internet as senhas mais comumente usadas. A combinação “123456” é seguidamente a campeã em termos de utilização. Seguida de perto por senhas tão inseguras como “senha”, “password” e “12345”.

Para quem possa imaginar que a presença de um caractere extra ou número não significa muito, é preciso considerar as seguintes disposições:

- a) uma senha de 6 caracteres somente com letras, tem 308.915.776 combinações possíveis;
- b) uma senha de 8 caracteres somente com letras, tem 208.827.064.576 combinações possíveis;
- c) uma senha de 8 caracteres com letras (maiúsculas e minúsculas) e que inclua números e símbolos, tem 6.095.689.385.410.816 de combinações possíveis.

Existe uma verdadeira força em números ou, neste caso, caracteres extras exigidos por senhas que estejam sob uma política de senhas fortes. É impor-

tante ressaltar que uma política de senha forte não precisa ser a única linha de defesa para seus sistemas e rede. Adicionar autenticação de fator múltiplo cria várias camadas de segurança para proteger usuários e recursos.

A autenticação de fator múltiplo é uma metodologia de segurança que requer mais de um método de autenticação de categorias independentes de credenciais para verificar a identidade do usuário para um *logon* ou outra transação. O conceito principal é combinar duas ou mais credenciais independentes. O objetivo é criar uma defesa em camadas e tornar mais difícil para uma pessoa não autorizada acessar um destino, como um local físico, um equipamento computacional, rede ou banco de dados. Se um fator é comprometido ou quebrado, o atacante ainda tem pelo menos mais uma barreira à violação antes de comprometer com sucesso o alvo. As categorias de fatores são descritas a seguir.

- ✖ **Fator de conhecimento:** informações que um usuário deve ser capaz de fornecer para efetuar *login*, ou seja, o que o usuário sabe. Isto inclui senhas, frases de segurança e PIN;
- ✖ **Fator de posse:** qualquer coisa que um usuário deve ter em sua posse para fazer *login*, ou seja, o que o usuário possui ou tem. Por exemplo, *token* de segurança, cartão de códigos numéricos, smartphone, entre outros;
- ✖ **Fator de herança:** quaisquer traços biológicos que o usuário tenha que possam ser confirmados para *login*, ou seja, o que o usuário é. Esta categoria inclui o escopo de métodos de autenticação biométrica, como íris, impressões digitais, varreduras de veias do dedo, reconhecimento facial, reconhecimento de voz, geometria da mão, entre outros.

Além dos três fatores principais outros dois fatores podem ser utilizados, sendo o fator de localização (localização atual do usuário através de um GPS), e o fator de tempo (por exemplo, não é possível que um cliente de banco utilize seu cartão de débito em São Paulo e 15 minutos depois, no Rio de Janeiro).

As boas senhas são críticas para a segurança da informação. A falta de boas práticas na criação de políticas de senha aumenta as chances de acesso

não autorizado ou dados comprometidos. Recomendamos que uma política de senha forte inclua as seguintes características:

- a) contenha uma combinação de letras maiúsculas, minúsculas, números e símbolos;
- b) contenha pelo menos oito caracteres;
- c) seja exclusiva, não sendo utilizada em mais de um serviço;
- d) não inclua palavras do dicionário;
- e) nunca inclua padrões de caracteres, por exemplo a sequência “qwerty” (sequência de teclado).

Além das características acima citadas, Lyra (2008) recomenda também que os sistemas possuam as seguintes regras relacionadas às senhas:

- ✗ **expiração da senha** – deve ser forçada a alteração das senhas dos usuários periodicamente;
- ✗ **repetições de senhas** – restringir, pelo menos, a utilização das últimas cinco senhas utilizadas recentemente;
- ✗ **quantidade de tentativas inválidas de acesso** – deve haver um limite para realizar o bloqueio das tentativas de acesso inválidas, de forma a evitar a descoberta das senhas. A boa prática sugere três tentativas;
- ✗ **troca de senhas iniciais (*default*)** – as senhas iniciais dos sistemas, banco de dados, ou quaisquer outros produtos, devem ser trocadas imediatamente, antes de sua utilização em ambiente de produção;
- ✗ **bloqueio automático por inatividade** – os sistemas devem possuir tempo máximo determinado para realizar o bloqueio / término de um acesso por inatividade do usuário;

3.11 Backup (cópias de segurança) e restore

Uma política de backup é uma programação predefinida em que as informações de aplicativos de negócios, bancos de dados de diversos servidores e arquivos de usuário são copiadas para um outro disco ou fita para garantir a disponibilidade e a integridade dos dados.

tir a recuperação dos dados no caso de perda acidental de dados e informações ou algum tipo de interrupção do sistema. As políticas normalmente terão um esquema de proteção padrão para a maioria dos servidores no ambiente, com políticas adicionais para determinados aplicativos ou dados críticos.

Por exemplo, uma política de backup padrão para todos os dados do aplicativo pode ser um backup noturno para a fita de segunda a sexta-feira, pelo qual um conjunto de fitas é mantido no local para facilitar a recuperação local e um segundo conjunto duplicado é enviado fora do local para armazenamento em um local seguro. Dados críticos de negócios podem ser protegidos por um conjunto de políticas adicionais. Nesta política pode constar que, além dos backups em fita noturnos, os dados instantâneos devem ser capturados e replicados em intervalos frequentes durante o dia útil para fornecer dados rápidos e granulares quando uma recuperação é necessária. Também podemos utilizar a tecnologia de *cloud computing* para backup, no entanto algumas recomendações de segurança devem ser observadas, conforme detalhamos em tópico subsequente.

De um modo geral as políticas de backup consistem em capturar um backup completo inicial de dados em disco e/ou fita, seguido de uma série de backups diários incrementais ou diferenciais.

Independentemente do método utilizado, no mínimo devem ser mantidas duas cópias de segurança – uma para permitir a recuperação no local e uma segunda em uma instalação segura, preferencialmente em um local físico separado (outro edifício, por exemplo). Dessa forma, se o *datacenter* for destruído por um desastre do tipo inundação, incêndio ou outro qualquer a cópia fora do local se torna o último recurso de recuperação.

3.11.1 Tipos de backup

A política de backup deve incluir, inicialmente, um backup completo. Um backup completo de dados consiste em fazer uma cópia completa de todos os dados de um determinado equipamento ou conjunto destes. Se ocorrer um evento de perda de dados, quanto mais recente for o backup completo, mais fácil será recuperar informações. Por esta razão, algumas organizações optam por executar tarefas de backup completas a cada noite. Entretanto, em alguns ambientes com grandes massas de dados os trabalhos de backup completos

levam mais de 24 horas para serem concluídos e consumirão muitos recursos de fita. Consequentemente, muitos administradores optam por executar um backup completo durante o fim de semana e executar backups incrementais ou diferenciais durante a semana para reduzir tanto a janela de backup noturno quanto economizar em mídia de fita.

Os backups **incrementais** realizam apenas backup dos dados que foram alterados desde a última tarefa de backup. Por exemplo, um backup incremental de segunda-feira após um backup completo de domingo só salvará os dados que foram alterados desde que o backup completo de domingo foi concluído. Da mesma forma, o backup incremental de terça-feira só irá fazer o backup dos dados que foram alterados desde o incremental de segunda-feira.

A melhor prática é usar fitas separadas e exclusivas para cada trabalho de backup incremental noturno. Isso garante alguma medida de redundância local se um cartucho de mídia de fita estiver com defeito ou for danificado durante o transporte.

Os backups **diferenciais**, por outro lado, farão backup de todos os dados que foram alterados desde o último backup completo. Por exemplo, o backup diferencial de quarta-feira abrange todos os dados que mudaram na segunda-feira, terça-feira e quarta-feira.

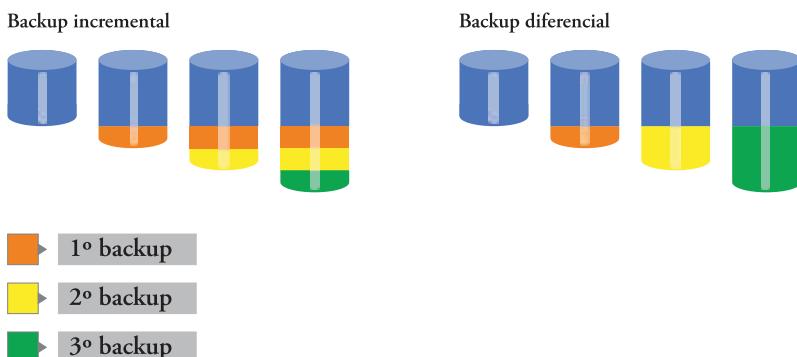
Como de costume, existem prós e contras para cada abordagem. Os backups incrementais podem ser concluídos com bastante rapidez e consumir apenas uma pequena quantidade de espaço de backup em comparação com backups completos ou diferenciais. Isso ajuda a reduzir janelas de backup e reduz o consumo de disco ou fita. Por outro lado, a recuperação é um processo um pouco mais complicado e demorado, porque mais fitas precisam ser carregadas para processá-las.

Os backups diferenciais removem alguns dos encargos de recuperação que podem ocorrer ao restaurar dados a partir de um backup incremental. No entanto, se o ambiente da aplicação estiver sujeito a mudanças frequentes de dados em uma rotina diária, a janela de backup pode se tornar alongada. Além disso, os diferenciais consumirão mais recursos de backup, uma vez que cada cópia de backup diferencial move e armazena todos os dados alterados desde o backup completo anterior.

Integrar solução em disco em uma arquitetura de backup é uma maneira ideal de remover algumas das complexidades do processo de backup e restauração. Nesse caso, não há nenhuma razão prática para não adotar uma política de backup incremental completa semanal e diária. Por exemplo, ao restaurar dados de backups incrementais salvos no disco, é eliminada completamente a necessidade de trocar vários cartuchos de fita para processar a recuperação.

A figura 3.5 exemplifica a diferença entre o backup incremental e o diferencial:

Figura 3.5 – Backup incremental *versus* diferencial



Fonte: Adaptada de <http://www.bbc.co.uk/education/guides/zws3gk7/revision/4>.

3.11.2 Políticas de backup

O objetivo das políticas de backup é garantir que existe um método consistente e confiável para recuperar dados. Políticas de backup *ad hoc*, como fornecer um compartilhamento de arquivo de rede para um usuário final, para que ele possa copiar seus dados mais críticos, devem ser analisadas com cautela. Caso ocorra negligência do usuário, há uma probabilidade muito alta de que dados críticos de negócios serão perdidos em algum momento no tempo e, muito provavelmente, a TI será responsabilizada.

Independentemente da arquitetura de backup implantada, o estabelecimento de políticas de backup regimentadas e claramente definidas é um bom primeiro passo para garantir a proteção consistente dos dados corporativos.

3.11.3 Testes de restauração (restore)

Todo bom plano de backup envolve testes de recuperação. É de extrema importância realizar ocasionalmente restaurações de teste nas mídias de backup. Em especial as mídias de fita porque as mesmas se desgastam e as unidades de fita ficam sujas ao longo do tempo. Os CDs podem ficar arranhados ou até embolorados, o que pode torná-los impossíveis de ler. Problemas de mídia não são a única razão para testar ocasionalmente a capacidade de restauração de dados de uma organização. Também tem a função de avaliar a funcionalidade dos procedimentos de backup adotados, bem como a capacitação da equipe de especialistas envolvidos.

Sistemas de backup *on-line* (ou backup em nuvem) não são exceção e devem ser testados também. A maioria dos provedores de serviços de backup *on-line* protege a empresa de estar diretamente exposto a problemas de mídia pela forma como eles usam sistemas de armazenamento tolerantes a falhas. Enquanto os sistemas de backup *on-line* são extremamente confiáveis, é necessário também testar o lado de restauração, para certificar-se de que não há problemas com a funcionalidade de recuperação, segurança ou criptografia. Este procedimento também é válido para o serviço de armazenamento em nuvem.

Existe diferença entre os serviços de armazenamento em nuvem e os serviços de backup em nuvem. O armazenamento é o serviço de guarda de arquivos, disponibilizando-os em qualquer dispositivo com acesso à internet. Se o arquivo for excluído do PC, por exemplo, ele será excluído dos outros dispositivos também. Já o backup em nuvem é o serviço de cópia de arquivos pessoais ou de uma organização, mantendo os seguros em caso de perda ou exclusão acidental dos mesmos. Outro diferencial do serviço de backup em nuvem é a possibilidade da criação de tarefas diárias, semanais ou mensais, possibilitando um histórico de modificação dos arquivos.

A lógica é efetuar backup de arquivos que um dia possam ser recuperados em caso de perda de dados. A propósito, perda de dados nunca ocorre em um momento conveniente. A maioria das vezes ocorre quando não há tempo hábil para lidar com o problema. Por isto é importante a etapa de recuperação estar bem consistente na política da empresa, pois a mesma necessita ser capaz de restaurar os arquivos perdidos rapidamente a fim de não comprometer o negócio. É melhor descobrir que o backup não possui qualidade em um momento em que não há ainda perda de dados.

3.12 Gerenciamento do uso e acesso a sistemas

Nos dias de hoje é comum que as organizações possuam informações que devem ser acessíveis a todos os usuários, informações que são necessárias para determinados grupos ou departamentos, bem como informações que devem ser acessados por apenas alguns indivíduos. Ter a informação centralizada em um sistema usado por todos contribui para o compartilhamento e o processamento de informações eficazes e rentáveis.

As informações que residem em um sistema que é acessado por muitos usuários, no entanto, também podem criar problemas. Uma preocupação significativa é assegurar que os usuários tenham acesso às informações de que necessitam, mas não tenham acesso inadequado a informações sensíveis. Também é importante garantir que alguns itens, embora possam ser lidos por muitos usuários, só possam ser alterados por alguns.

Controles de acesso lógico são o meio de resolver estes problemas. Os controles de acesso lógico são mecanismos de proteção que limitam o acesso dos usuários à informação e restringem suas formas de acesso no sistema somente ao que é apropriado para eles. Os controles de acesso lógico são frequentemente incorporados ao sistema operacional ou podem ser parte da “lógica” de aplicativos ou utilitários principais, como os Sistemas de Gerenciamento de Banco de Dados (SGBD). Também podem ser implementados a nível de sistema operacional. Além disso, os controles de acesso lógico podem estar presentes em componentes especializados que regulam as comunicações entre computadores e redes.

Faremos uma breve explanação de formas comuns de controle de acesso lógico disponíveis atualmente nos próximos tópicos.

3.12.1 Modos de acesso

O conceito de modos de acesso é fundamental para o controle de acesso lógico. O efeito de muitos tipos de controle de acesso lógico é permitir ou negar o acesso de indivíduos específicos a recursos de informações específicos em modos de acesso específicos. Segue uma introdução aos modos de acesso comumente utilizados:

- × **somente leitura** – isso fornece aos usuários a capacidade de exibir, copiar e geralmente imprimir informações, mas não permitindo alterá-las de qualquer maneira, como excluir, adicionar ou modificar.
- × **escrita** – os usuários têm permissão para visualizar e imprimir, bem como adicionar, excluir e modificar informações. O controle de acesso lógico pode refinar ainda mais a relação de leitura / gravação de modo que um usuário tenha capacidade de somente leitura para um campo de informações, mas a capacidade de escrever em um campo relacionado.
- × **executar** – a atividade mais comum realizada pelos usuários em relação aos programas de aplicativos em um sistema é executá-los. Um usuário executa um programa cada vez que ele ou ela usa um processador de texto, planilha, banco de dados, etc.

A figura 3.6 exemplifica o relacionamento entre estes três modos de acesso. É possível criar permissões híbridas que incluem um ou mais modos (*read* – somente leitura, *write* – escrita, *execute* – executar).

Figura 3.6 – Modos de acesso



Fonte: Adaptado de Shutterstock.com/LOVEgraphic.

3.12.2 Outras restrições

Além das restrições baseadas no modo de acesso, os controles de acesso lógico podem negar ou permitir o acesso com base em outros fatores. Por exemplo, o acesso pode ser permitido somente durante determinadas horas do dia, ou apenas a partir de terminais ou locais de rede específicos. Ou também o acesso pode ser permitido seletivamente com base no tipo de serviço solicitado.

3.12.3 Relacionamento com identificação e autenticação

Processo pelo qual qualquer pessoa que tenta interagir com um sistema estabelece sua identidade com o sistema, por exemplo, usando uma senha ou *token*. O processo de controle de acesso lógico então associa as informações apropriadas e formas permissíveis de acessos com essa identidade fornecida.

3.12.4 Administração de controle de acesso lógico

A administração é o aspecto mais complexo e desafiador do controle de acesso lógico. A administração de controles de acesso lógico envolve a implementação, monitoramento, modificação, teste e encerramento de acessos de usuários no sistema e pode ser uma tarefa exigente.

As decisões reais sobre quem pode ter acesso a determinados recursos geralmente são responsabilidade do proprietário dos dados, fazendo-as em conjunto com a área de gestão.

Existem três abordagens básicas para a administração que implementa estes controles: centralizada, descentralizada ou uma combinação entre elas. Cada um tem vantagens e desvantagens relativas, e o que é melhor dependerá das necessidades e da complexidade da organização em particular:

- ✖ **administração centralizada** – um elemento (geralmente um grupo em grandes organizações e um indivíduo em pequenas) é responsável pela configuração de controles de acesso. A principal vantagem é que um controle muito rigoroso sobre as informações pode ser mantido porque a capacidade de fazer alterações reside em um

número muito reduzido de pessoas. Uma desvantagem importante, porém, é que o processo de mudança pode ser constante, tornando a tarefa de administração demorada e dispendiosa em termos de pessoal e equipamentos.

- × **administração descentralizada** – significa que o acesso à informação é controlado pelos proprietários ou criadores dos arquivos. A vantagem é que o controle está nas mãos dos indivíduos mais responsáveis pela informação, mais familiarizados com ela. A desvantagem, no entanto, é que pode não haver consistência entre os proprietários/criadores quanto aos procedimentos e critérios para a concessão de acessos e capacidades dos utilizadores.
- × **abordagem híbrida** – em uma abordagem híbrida, o controle centralizado é exercido para alguns tipos específicos de informações e o descentralizado é permitido para outras informações. Procura reunir as vantagens das duas primeiras, de forma que o melhor resultado seja encontrado.

3.12.5 Superusuários

Independentemente do tipo de administração escolhido, as necessidades prevalecentes de acesso adequado ao usuário, além da manutenção da segurança do sistema de TI, precisam ser asseguradas. Para contribuir para atender a essas necessidades, todos os esquemas de controle de acesso lógico permitem recursos de “superusuário” para um indivíduo ou grupo pequeno. Isso permite que todas as atividades de usuário e administrador sejam alteradas ou substituídas imediatamente quando necessário. Além disso, superusuários normalmente têm capacidades para acessar e interagir com programas críticos do sistema, como o sistema operacional, não acessível por outros. Este tipo de acesso é necessário para manutenção e *upgrades*, por exemplo.

Como os superusuários têm privilégios suficientes para ignorar ou modificar os controles de acesso lógico, os recursos de superusuário apresentam uma vulnerabilidade potencial e devem ser cuidadosamente protegidos. As organizações devem minimizar rigorosamente o número de indivíduos que estão autorizados a atuar como superusuários. Além disso, precauções adicionais como garantir que as senhas dos superusuários sejam

robustas e alteradas regularmente, são importantes para minimizar as oportunidades para indivíduos não autorizados obterem acesso de superusuário aos sistemas.

3.12.6 Custos

A incorporação de controle de acesso lógico em um sistema de TI envolve tanto a compra ou utilização de mecanismos de controle de acesso como uma mudança de comportamento por parte dos usuários.

Entre os **custos diretos** associados ao uso de métodos de controle de acesso lógico estão a compra e suporte de hardware, sistemas operacionais e aplicativos que fornecem os controles e quaisquer pacotes de segurança adicionais necessários ou desejáveis. O custo de pessoal mais significativo em relação ao controle de acesso lógico é geralmente para administração. A maioria dos sistemas operacionais multiusuários fornecem algum mecanismo de proteção, portanto há menos custo de aquisição associado a estes. Treinar usuários para entender e usar um sistema de controle de acesso lógico é um custo muito necessário. Se os usuários não estão confortáveis em usar um sistema de controle de acesso, eles tentarão configurá-lo de um modo com poucas ou nenhuma restrição. Isso pode proporcionar à organização uma falsa confiança na segurança de seus recursos de TI, resultando em uma situação de segurança pior do que se os mecanismos de proteção não tivessem sido fornecidos em primeiro lugar.

O principal **custo indireto** associado à introdução de controles de acesso lógico em um sistema de TI é o efeito sobre a produtividade do usuário. Há duas dimensões principais para esta situação: A primeira é a sobrecarga adicional que os usuários individuais têm ao determinar corretamente (quando está sob seu controle) os atributos de proteção das informações. Esta determinação requer tanto uma compreensão da política relevante que rege o tratamento da informação como uma compreensão da tecnologia que suporta o controle de acesso lógico. A outra dimensão centra-se na situação dos usuários que não conseguem acessar as informações necessárias para seus trabalhos porque as permissões foram atribuídas incorretamente. Embora infrequente, esta situação é familiar para a maioria das organizações que colocam ênfase forte no controle de acesso lógico.

3.13 Segurança no tratamento de mídias

Estudamos as normas da família ISO 27000 no capítulo anterior. Existem seções da norma que fornecem orientações sobre como descartar de forma segura mídias de armazenamento de maneira que minimizem os riscos de expor informações comprometedoras.

O descarte de mídias pode parecer uma atividade simples, uma vez que, em geral, apenas descartamos coisas que consideramos não mais necessárias ou não valiosas. No entanto, pensando em atividades de reciclagem ambiental, pode-se perceber que o que é inútil para alguém pode ser altamente valioso para outra pessoa. O mesmo se aplica às informações. Algumas informações que consideramos não valiosas podem levar um concorrente a obter uma vantagem comercial, um criminoso pode explorar as fraquezas de uma organização ou, pior, causar danos à vida pessoal de um cliente ou de um colaborador, usando informações pessoais ou privadas para cometer um crime.

Com o objetivo de proteger as informações relevantes de uma empresa durante todo o seu ciclo de vida, é necessário estar atento a dois controles específicos relacionados ao descarte de informações:

- a) sempre que uma mídia de armazenamento seja descartada, deve-se considerar o uso de procedimentos para assegurar a eliminação adequada da informação.
- b) os equipamentos que contêm mídias de armazenamento devem ser verificados para garantir que estejam isentos de informações sensíveis antes da eliminação ou reutilização.

No que diz respeito à eliminação de mídias de armazenamento, os procedimentos de eliminação devem ser proporcionais ao nível de classificação da informação: Quanto maior a classificação, maior deverá ser a garantia de que as informações não podem ser recuperadas após a eliminação. Uma das boas práticas, no caso de discos rígidos (HDD), é a utilização de ferramentas de formatação de baixo nível (que efetuam sobrescrita de todo o disco). Para o caso de papel utilizar um equipamento triturador.

Para garantir que os itens foram descartados corretamente, é necessário também manter informações de registro listando, no mínimo, quem realizou o procedimento, quando e qual método foi usado para o descarte, para fins de auditoria futura.

Outro item que exige atenção é o transporte de mídias com informações classificadas. É necessário definir os seguintes requisitos mínimos para tal processo (FERREIRA, 2008).

- a) Relação formal, por meio de contratos, com os portadores;
- b) Recipientes lacrados;
- c) Escolta armada por segurança patrimonial;
- d) Monitoração de veículos por satélite;
- e) Utilização de senhas, criptografia e assinatura digital.

3.14 Governança de segurança da informação

Governança é um termo que remete a governo, autoridade e controle. Governança corporativa é o meio pelo qual as sociedades empresariais são dirigidas e monitoradas pelos seus proprietários e/ou acionistas. A área de governança de TI começou a ganhar força nas últimas décadas, sendo uma espécie de ponte entre a área de TI e o restante da organização. Segundo Ferreira (2008) a boa governança possui as seguintes características.

- a) Participação;
- b) Estado de direito (regido por normas previamente definidas);
- c) Transparência;
- d) Responsabilidade;
- e) Orientação por consenso;
- f) Igualdade e inclusão;
- g) Efetividade e eficiência;
- h) Responsabilização (do inglês: *accountability*).

Dentro deste conceito de governança, a segurança da informação afeta toda a organização ou negócio da empresa. A governança de segurança da informação passa a ser definida como

a prática que garante que o tema segurança da informação é adequadamente tratado em consonância com os requerimentos exigidos pelas

partes envolvidas no processo, com o respectivo mapeamento de riscos ao ativo informação das organizações, estrutura de gestão, de suporte, divulgação, resposta a incidentes, reporte, cobertura dos aspectos de TI e monitoramento contínuo (FERREIRA, 2008, p. 185).

A seguir listamos os pontos chaves de um processo de governança de segurança da informação.

- a) Respostas às preocupações da alta administração da organização;
- b) Considerações e preocupações dos administradores de Tecnologia e Segurança da Informação;
- c) Plano e programa de segurança da informação baseado em princípios estabelecidos;
- d) Iniciativas de segurança da informação;
- e) Fontes de conhecimento para o processo de segurança da informação;
- f) Critérios para medição da performance de segurança da informação;
- g) Avaliação geral da função de segurança da informação.

3.15 Gerenciamento e segurança em ambientes na nuvem (cloud computing)

Nos últimos anos a computação em nuvem (*cloud computing*) ganhou cada vez mais força e várias organizações tornaram-se adeptas desta solução. Existem muitas vantagens da computação em nuvem, entre elas podemos citar o menor custo, incremento de mobilidade e menor impacto ambiental. No entanto, a segurança dos dados na nuvem é uma preocupação fundamental para os departamentos de TI.

A segurança da computação em nuvem é o conjunto de tecnologias e políticas baseadas em controles, em conformidade com os regulamentos vigentes a fim de proteger as informações, os aplicativos de dados e a infraestrutura associados ao uso desta solução.

Devido à própria natureza da nuvem como um recurso compartilhado, o gerenciamento de identidade, privacidade e controle de acesso são uma pre-

ocupação particular. Com mais organizações usando esta solução a segurança adequada nessas e em outras áreas potencialmente vulneráveis tornou-se uma prioridade para as organizações que contratam um provedor de serviços de dados em nuvem.

Os processos de segurança de computação em nuvem devem abordar os controles de segurança que o provedor incorporará para manter a segurança dos dados do cliente. Os processos também provavelmente incluirão um plano de continuidade de negócios e um plano de backup de dados no caso de uma violação de segurança na nuvem.

Listamos a seguir os principais cuidados que os administradores de TI devem avaliar quando se trata de contratar serviços de computação em nuvem.

- ✖ **Disponibilidade de rede:** a conectividade de rede e a largura de banda devem atender às suas necessidades mínimas da organização;
- ✖ **Viabilidade do provedor:** deve ser avaliado o grau de confiança que o provedor apresenta;
- ✖ **Recuperação de desastres e continuidade de negócios:** deve haver um planejamento claro se o ambiente de produção do provedor de nuvem estiver sujeito a um desastre;
- ✖ **Incidentes de segurança:** o provedor deve informar sobre qualquer violação de segurança;
- ✖ **Transparência:** o provedor deve expor detalhes de sua própria política ou tecnologia interna.

Síntese

Neste capítulo aprendemos como podemos transformar recomendações presentes em normas de segurança da informação em aplicações práticas em ambientes de TI. Vimos que a equipe de TI deve ser responsável pela conscientização quanto ao uso responsável dos recursos computacionais de uma organização.

Aprendemos também como a segurança física de ambiente, em especial quanto ao *Datacenter* e a segurança lógica contribuem para garantia dos aspectos fundamentais da segurança de informação.

As tecnologias como *firewalls*, IDS, IPS e DMZ contribuem significativamente para tal garantia, bem como as políticas implementadas pelos administradores, fundamentais para os usuários sejam conscientizados a respeito de seus limites e responsabilidades quanto ao uso dos recursos de TI.

Atividades

1. Explique resumidamente como o IPv6 melhora os aspectos de segurança ausentes no IPv4.
2. Explique resumidamente como funciona uma rede de perímetro (DMZ).
3. Quais são os fatores de autenticação envolvidos em um *login*, onde um usuário necessita digitar uma senha e um código numérico recebido em seu smartphone?
4. Qual a diferença entre backup incremental e backup diferencial?

4

Aspectos Tecnológicos da Segurança da Informação

No CAPÍTULO ANTERIOR, detalhamos os principais procedimentos e boas práticas que um administrador deve implementar para garantir a segurança da informação em uma organização. Neste capítulo, iremos aprofundar os estudos sobre os aspectos tecnológicos da segurança da informação, compreendendo melhor os conceitos de software malicioso e ferramentas de proteção contra este. Também aprofundaremos os aspectos técnicos que devem ser observados pelos desenvolvedores de software, para que as aplicações sejam desenvolvidas de forma a não deixar a segurança de lado. Ainda, estudaremos os pontos principais que devem ser parte de uma aquisição segura e gerenciamento de utilização de aplicativos.

TERMINAREMOS O ESTUDO deste capítulo compreendendo o funcionamento da criptografia, do certificado e da assinatura digital, que são aspectos tecnológicos fundamentais na garantia da segurança da informação.

Objetivo de aprendizagem:

- × Compreender aspectos tecnológicos fundamentais para a segurança da informação.

4.1 Software malicioso

Malware, abreviação do termo original em inglês *malicious software*, ou “software malicioso”, refere-se a um tipo de programa de computador projetado para infectar o computador de um usuário legítimo e infligir danos neste equipamento de várias maneiras. Existem diferentes tipos de *malware* que contêm características únicas e comportamentos diferentes.

Muitos usuários de computadores consideram *malware*, vírus, *spyware*, *adware*, *worms*, *trojans*, entre outros termos, como a mesma coisa. E, embora todas essas infecções prejudiquem nossos computadores, elas possuem características peculiares. Os significados de muitas dessas palavras mudaram ao longo do tempo, porém para facilitar nosso entendimento classificaremos em duas categorias: como o *malware* infecta o seu sistema (método de infecção); e qual o comportamento do *malware* uma vez que está ativo em um sistema.

A primeira categoria (método de infecção) diz respeito a dois fatores principais: como o *malware* entrou no sistema e como ele continua a propagar-se. O *malware* geralmente se encaixa em uma das seguintes categorias:

- × **vírus** é um termo que costumava ser genérico para qualquer software malicioso até a última década. No entanto, atualmente é usado o termo “*malware*” para este conceito genérico. A palavra “vírus” é utilizada para descrever um programa que se autorreplica após alguma ação do usuário (por exemplo, a abertura de um anexo de e-mail infectado).
- × **worm** é outro tipo de programa autorreplicante, mas diferente dos vírus, ele não necessita de uma intervenção do usuário para tal. Os *worms* costumam ocupar bastante banda de rede, interferindo no funcionamento da mesma, pois costumam vasculhar a rede por vulnerabilidades que possam ser exploradas em outros computadores e sistemas.

- ✖ **Trojan horse** é um programa que aparenta ser inofensivo, mas que contém ou instala um outro programa malicioso (o *trojan*). O termo é derivado do mito clássico do cavalo de Troia que aparenta ser útil ou interessante, mas é realmente prejudicial quando executado. Uma subcategoria são os *trojans* de acesso remoto (RAT), ou **backdoor**, cujo objetivo é criar uma porta de entrada secreta em um sistema infectado, de modo que permita a invasores acessarem este sistema remotamente de forma mais fácil futuramente.
- ✖ **drive-by download** é provavelmente a forma mais popular de infecção de computadores. Na maioria das vezes, ocorre ao visitar um endereço da internet infectado. A página infectada explora uma vulnerabilidade do navegador ou *plugin*, executando um código malicioso e realizando a infecção.

A segunda categoria diz respeito às várias ações que o *malware* pode tomar, uma vez estando no sistema. Por vezes tentará replicar-se sem danos visíveis, mas outras vezes efetuará ações que provocarão grandes danos. Tais ações podem enquadrar-se normalmente em um dos aspectos abaixo listados:

- ✖ **adware** é um *malware* menos perigoso pois sua função é exibir publicidade ao usuário, a maioria das vezes de forma indesejada. Alguns *adwares* efetuam o rastreamento da máquina do usuário. Na maioria das vezes, são instalados juntamente com outros softwares úteis, nas opções de instalação padrão. Geralmente, pode ser removido pela desinstalação do software ao qual ele foi anexado.
- ✖ **spyware** é um programa que monitora o computador do usuário e revela informações coletadas a uma parte terceira interessada.
- ✖ **ransomware** é um programa malicioso que tornou-se muito popular entre os criminosos virtuais que procuram perceber valores monetários. Trata-se do “sequestro de dados”, onde pastas do sistema operacional infectado serão criptografadas, impossibilitando seu acesso normal. Em seguida, será exibida uma mensagem que exige alguma forma de pagamento para que o usuário possa obter a chave que descriptografa os arquivos.

- ✗ **scareware** é um programa que quando executado exibe uma mensagem assustadora ao usuário, informando que seu sistema encontra-se infectado ou com falhas de registro. O software afirma ser capaz de corrigir os problemas encontrados se o usuário efetuar o pagamento do mesmo.

Saiba mais

Outro termo conhecido também é o **rootkit**. Trata-se de um programa malicioso (ou conjunto de programas) que altera arquivos de características administrativas do sistema operacional de modo a ficar invisível, para manter uma presença persistente e indetectável na máquina. Uma vez instalado, um invasor pode executar praticamente qualquer função no sistema para incluir acesso remoto, espiãgem, bem como ocultar processos, arquivos, chaves de registro e canais de comunicação.

4.2 Proteção contra software malicioso

Os programas de proteção contra software malicioso (antivírus) são projetados para detectar, prevenir e remover software malicioso de um sistema. No seu núcleo, o software antivírus fornece detecção baseada em assinaturas de *malware*. Uma assinatura de vírus é baseada em um segmento único de código-fonte dentro do *malware*. Quando um usuário atualiza as definições de vírus de um software antivírus significa que novas assinaturas antes desconhecidas foram inseridas no banco de dados local da aplicação.

Desde o seu início, no final da década de 1980, o software antivírus evoluiu junto com as ameaças das quais ele protege. Como resultado, a detecção de assinatura estática de hoje (correspondência de padrões) é frequentemente reforçada com tecnologias de prevenção de intrusão ou comportamentais mais dinâmicas.

O tema mais comum quando o assunto é antivírus, é a discussão sobre produto gratuito versus pago. Existem pacotes de distribuição com vários formatos, desde *scanners* antivírus autônomos a suítes completas de segurança

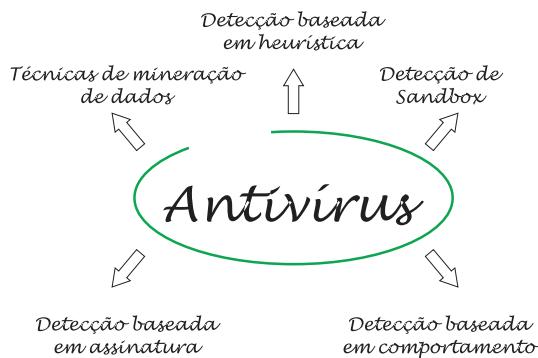
de internet que agregam antivírus com um *firewall*, controles de privacidade e outras proteções de segurança complementares, como proteção de e-mail. Alguns fornecedores de renome oferecem software antivírus gratuito para uso doméstico (às vezes, estendendo-os para *Small Office and Home Office* – também conhecidos pela sigla SOHO).

Análises sugerem que os produtos pagos tendem a demonstrar níveis mais elevados de prevenção e remoção do que produtos gratuitos. Por outro lado, o produto gratuito por ser menos rico em recursos, consome menos recursos do sistema, o que sugere que ele pode funcionar melhor em computadores mais抗igos ou em computadores com capacidade limitada de processamento. Também é característico de softwares *Open Source* a disponibilização mais ágil de atualizações e melhorias, visto que a comunidade de desenvolvedores é, via de regra, maior.

Soluções gratuitas são recomendadas apenas para usuários domésticos. Para ambientes corporativos é recomendável a compra de soluções de antivírus mais robustas, que incluem controle centralizado de atualizações e monitoramento constante de máquinas clientes da rede.

Existem cinco formas de detecção que os softwares antivírus utilizam para melhorar a sua eficiência de funcionamento, apresentados na figura a seguir.

Figura 4.1 – Formas de detecção de um antivírus



Fonte: Shutterstock.com/arka38.

- × **Signature-based detection** (detecção baseada em assinatura): é a forma mais comum utilizada pelos softwares antivírus, que verifica

todos os arquivos executáveis (.exe), confrontando-os com a lista conhecida de assinaturas de vírus e outros tipos de *malware*.

- × **Heuristic-based detection** (detecção baseada em heurística): este tipo de detecção é a mais comumente usada em combinação com detecção baseada em assinatura. A tecnologia heurística funciona na maioria dos programas antivírus distribuídos atualmente. Esta técnica auxilia o software antivírus a detectar variantes de um *malware*, mesmo na ausência das definições de vírus mais recentes.
- × **Behavioral-based detection** (detecção baseada em comportamentos): este tipo de detecção é usado em mecanismos de Detecção de Intrusão. Caracteriza-se por focar mais na detecção das características conhecidas que um programa malicioso realiza durante a sua execução.
- × **Sandbox detection** (detecção “caixa de areia”): tem um funcionamento parecido com a detecção de comportamento. A diferença é que o usuário tem a opção de executar um programa na “sandbox”, que é um ambiente virtualizado isolado do resto do sistema operacional. Verificando as ações que o programa realiza, o software antivírus pode identificar se o programa é mal-intencionado ou não, sem risco de infectar o sistema operacional.
- × **Data mining techniques** (técnicas de mineração de dados): esta é uma das últimas tendências na detecção de um *malware*. Com um conjunto de recursos do programa, a mineração de dados do sistema ajuda a descobrir se o programa é malicioso ou não.

Ferreira (2008) destaca quatro pontos principais para proteger uma organização contra a infecção por *malwares*, listadas a seguir:

- a) uso obrigatório de software antivírus em todos os equipamentos;
- b) atualização periódica das definições de vírus e versão do produto;
- c) verificação de todo arquivo recebido anexado em e-mail, ou download, pela solução de antivírus;
- d) disponibilização de treinamento adequado que oriente a utilização do software de antivírus para os usuários.

As soluções de antivírus que devem ser adotadas pelos administradores de TI nas organizações dependem, em boa parte, do tamanho da mesma. Organizações muito pequenas com apenas alguns computadores podem instalar soluções de antivírus individualmente em cada equipamento. Organizações com 10 a 20 computadores devem considerar a utilização de um conjunto de segurança, incluindo uma solução que permita a administração do software de maneira centralizada, ao invés de lidar com cada computador separadamente. Já organizações com mais de 20 computadores devem considerar ferramentas de nível empresarial que, além de permitirem a administração centralizada de atualizações de definição e outras tarefas, fornecem também ferramentas de segurança adicionais apropriadas para grandes organizações.

4.3 Segurança no desenvolvimento de software

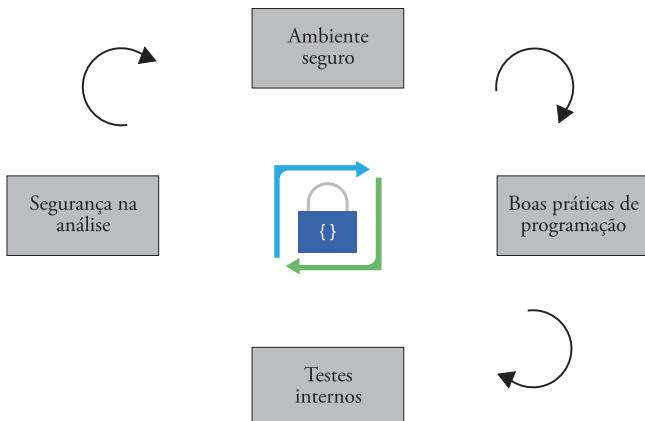
É de fundamental importância que sejam seguidos procedimentos que possam garantir a segurança no processo de desenvolvimento de software. Uma das principais normas existentes atualmente que permite especificar a segurança de uma aplicação de forma clara, a partir de características do ambiente e da aplicação, é a ISO/IEC 15408, também conhecida como *Common Criteria*. Esta norma pode ser utilizada tanto para desenvolver um sistema seguro como também para avaliar a segurança de um sistema já existente.

O *Common Criteria* tem dois componentes chave: O *Security Target* (objetivo ou alvo de segurança), o qual indica quais aspectos de segurança foram considerados importantes para aquele sistema em particular. E o *Evaluation Assurance Level – EAL* (Nível de Garantia de Avaliação) que define níveis de garantia de segurança. Estes níveis são escalados de um a sete, sendo o primeiro nível contendo menos rigor no teste, portanto com menor garantia de que o sistema atende os requisitos de segurança. O último nível de maturidade e segurança envolve muito esforço de programação e altos recursos de investimento. A literatura apresenta o nível três como significativamente seguro para a maioria dos sistemas comerciais.

Lyra (2008) apresenta um modelo simplificado para utilização da norma ISO/IEC 10.408, de forma a garantir que a maioria dos sistemas comerciais seja desenvolvida com parâmetros que implementem segurança na aplicação.

Para sistemas que ainda estão **em processo de desenvolvimento**, apresentamos as etapas na figura a seguir:

Figura 4.2 – Etapas do processo de desenvolvimento de software seguro



Fonte: Elaborada pelo autor.

As etapas consistem em:

- ✗ **segurança na análise** – deve ser especificada a segurança da aplicação na fase de análise, usando a norma *Common Criteria* como guia.
- ✗ **ambiente seguro** – o ambiente de desenvolvimento e testes deve ser capaz de atender ao EAL3 da norma, considerado seguro para a maioria das aplicações comerciais.
- ✗ **boas práticas de programação** – deve ser criado um processo de desenvolvimento bem definido seguindo os requisitos de segurança. Detalharemos boas práticas de programação no tópico 4.5.
- ✗ **testes internos** – os testes devem gerar evidências de que o sistema atende às especificações do EAL3.

Saiba mais

Para aplicações que já estão desenvolvidas a norma pode ser adaptada de modo que seja realizado o levantamento dos requisitos de

segurança que a aplicação possui, realizando a sua classificação de acordo com o nível de garantia de segurança (EAL), de um a três. Para os níveis acima de quatro até sete é necessário que sejam realizados testes e procedimentos durante o processo de desenvolvimento, portanto não se aplicam a sistemas já desenvolvidos.



4.4 Segurança do ambiente de desenvolvimento

Somente é possível desenvolver aplicações seguras dentro de um ambiente seguro. As normas relacionadas à segurança da informação aliadas ao desenvolvimento (ISO/IEC 15.408 e família ISO/IEC 27000) devem servir como base ao desenvolvedor que necessita garantir a segurança de suas aplicações. Lyra (2008) elenca sete aspectos fundamentais que devem fazer parte de um ambiente seguro de desenvolvimento:

- ✖ **gerência de configuração** – tem por objetivo tornar o processo de desenvolvimento menos suscetível a erros ou negligencia humana, prevenindo mudanças, acréscimos e exclusões desautorizadas na documentação do sistema.
- ✖ **distribuição** – refere-se à etapa de transição entre o desenvolvimento e a produção, assegurando que a versão disponibilizada para implantação apresenta os atributos de segurança especificados.
- ✖ **desenvolvimento** – as funcionalidades de segurança devem ser representadas em seus vários níveis de abstração, desde o projeto lógico até a implementação de seus produtos finais.
- ✖ **documentação** – deve ser bem completa de forma que os usuários sejam conscientizados das funcionalidades de segurança, bem como os administradores do sistema, para operação segura do mesmo.
- ✖ **suporte ao ciclo de vida** – devem ser adotados modelos de ciclo de vida reconhecidos por especialistas (CMMI, RUP, etc.). A adoção de tais modelos auxilia na garantia de que os aspectos relaciona-

dos à segurança sejam tratados adequadamente durante o ciclo de desenvolvimento e manutenção.

- × **testes de segurança** – entre os testes que visam garantir que o sistema atenda aos requisitos funcionais de segurança podemos citar os testes de unidade, de integração, de instalação e de aceitação.
- × **avaliação de vulnerabilidades** – os testes de vulnerabilidades devem ser conduzidos de forma a abranger as ameaças passíveis de exploração, possibilidade de mau uso do sistema e falha dos mecanismos de segurança.

4.5 Boas práticas de programação

Em um ambiente cada vez mais dinâmico e complexo de ameaças atualmente, é necessário que os desenvolvedores empreendam esforços significativos para reduzir vulnerabilidades, melhorar a resistência aos ataques e proteger a integridade das aplicações desenvolvidas.

Existem práticas de programação que podem ser aplicadas em diversos ambientes de desenvolvimento para melhorar a segurança do aplicativo desenvolvido. Estas práticas devem ser aplicadas em cada estágio do processo de desenvolvimento: requisitos, design, programação, testes, manuseio de código e documentação.

A produção de código seguro na maioria das vezes produz queda de performance, porém é preferível assumir o custo de um tempo maior de desenvolvimento frente ao prejuízo de perdas decorrentes de incidentes em aplicações não-seguras.

A seguir elencaremos algumas recomendações de boas práticas fornecidas por vários autores especialistas no assunto.

4.5.1 Operar com menos privilégio

O conceito de manusear o código com um conjunto mínimo de privilégios é tão válido hoje como era há 30 anos. O conceito de privilégio mínimo é simples, mas pode ser difícil de ser implementado em alguns casos. Mesmo que “menos privilégio” signifique coisas diferentes em ambientes diferentes,

o conceito é o mesmo: cada programa e cada usuário do sistema deve operar usando o menor conjunto de privilégios necessários para concluir o trabalho.

Operar com menos privilégio é importante porque pode ajudar a reduzir os danos causados se um sistema for comprometido. Um aplicativo comprometido executado com privilégios completos pode executar mais danos do que um aplicativo comprometido executado com privilégios reduzidos.

O conceito de privilégio varia de acordo com o sistema operacional, as tecnologias de desenvolvimento e os cenários de implantação. Privilégios, capacidades e direitos determinam quais operações sensíveis podem ser realizadas por aplicativos e usuários. No interesse da segurança, é imperativo que as operações sensíveis sejam reduzidas ao mínimo.

Há dois aspectos de desenvolvimento com privilégio mínimo que devem ser considerados. O primeiro é certificar-se de que o aplicativo opera com privilégios mínimos e o segundo é testar o aplicativo totalmente em um ambiente de privilégio mínimo. É altamente recomendável que todos os desenvolvedores e testadores criem e testem aplicativos usando contas de privilégios menores.

Deve-se também testar completamente o aplicativo em um ambiente de privilégio mínimo para eliminar os bugs relacionados a este ambiente. Recomenda-se que a aplicação em teste seja sujeita a um teste completo e todas as questões relacionadas à segurança sejam anotadas e corrigidas.

Finalmente, é necessário realizar auditorias ou revisões regulares das permissões padrão, para que isso seja um meio eficaz de garantir privilégios mínimos no código.

4.5.2 Minimizar o uso de strings inseguras e funções de buffer

Vulnerabilidades de corrupção de memória, como *buffer overruns*, são comuns em aplicativos escritos em linguagem C e C++. Um exemplo de função intrinsecamente insegura é a *strcpy*. Os engenheiros de desenvolvimento devem ser instruídos a evitar o uso dessas classes de chamadas de função. Usar ferramentas para pesquisar o código por estas chamadas ajuda a verificar se os desenvolvedores estão seguindo as orientações bem como identificar também

problemas no início do ciclo de desenvolvimento. Existem funções de substituição que podem ser utilizadas, como exemplo citamos as funções contidas no quadro 4.1 a seguir:

Quadro 4.1 – Funções inseguras e sua equivalente segura

Função Insegura	Função Segura
strcpy	strcpy_s
strncpy	strncpy_s
strcat	strcat_s
strncat	strncat_s
scanf	scanf_s
sprintf	sprintf_s
memcpy	memcpy_s
gets	gets_s

Fonte: <https://www.safecode.org/>.

4.5.3 Tratar entrada e saída de dados

Verificar a validade dos dados recebidos e rejeitar dados em não-conformidade pode remediar as vulnerabilidades mais comuns que levam a incidentes de segurança. Em alguns casos, verificar a validade dos dados não é um exercício trivial, no entanto, é fundamental para mitigar os riscos de vulnerabilidades mais comuns em aplicativos.

Verificar a validade dos dados de saída pode remediar muitas vulnerabilidades baseadas em aplicativos *web*, como *scripts* entre sites, bem como atenuar os problemas de vazamento de informações.

A validação de entrada refere-se à verificação da validade dos dados antes de ser processada pela aplicação, enquanto que a validação da saída refere-se a validação dos dados da aplicação depois de processada, com o propósito de corresponder às expectativas do destinatário.

Podem ser utilizadas estratégias de lista branca *versus* lista negra para mitigar os riscos durante entrada e saída de dados. As listas brancas tipica-

mente restringem as entradas do aplicativo a uma lista de valores pré-selecionados, enquanto a lista negra dá mais liberdade e rejeita apenas os elementos e / ou tipos de dados banidos.

A validação de dados também não deve ser negligenciada para aplicativos que trocam dados com outras aplicações sem interação do usuário.

4.5.4 Evitar concatenações de strings para cláusulas de SQL dinâmicas

A criação de instruções SQL é comum em aplicativos orientados a banco de dados. Infelizmente, a maneira mais comum e perigosa de criar instruções SQL é concatenar dados não confiáveis com constantes de *string*. Exceto em casos muito raros, a concatenação de *string* não deve ser usada para construir instruções SQL. O uso de *stored procedures*, criptografia de banco de dados, SSL e a remoção e duplicação de aspas simples como formas de corrigir vulnerabilidades de injeção de SQL podem dificultar um ataque, bem como o uso apropriado de cláusulas SQL.

A configuração correta do banco de dados é um mecanismo vital de defesa em profundidade e não deve ser ignorada. A princípio, somente *stored procedures* específicas devem ter permissão de execução e não devem fornecer acesso direto a tabelas do banco. As contas do sistema que atendem a solicitações de banco de dados devem ter o privilégio mínimo necessário para o aplicativo ser executado. Se possível, o mecanismo de banco de dados deve ser configurado para suportar apenas consultas parametrizadas.

Os ataques de injeção SQL bem-sucedidos podem ler dados confidenciais, modificar dados e até mesmo executar comandos a nível de sistema operacional.

4.5.5 Evitar o uso de criptografia fraca

Nos últimos anos, graves deficiências foram encontradas em muitos algoritmos criptográficos. Devido ao uso generalizado da criptografia para garantir a autenticação e autorização em sistemas as deficiências relacionadas com a criptografia podem ter um sério impacto na segurança de uma aplicação.

Os seguintes algoritmos e tecnologias criptográficas devem ser tratados como inseguros: MD4, MD5, SHA1 e algoritmos criptográficos simétricos com uso de chaves menores que 128 bits.

É importante também que não sejam armazenadas em código-fonte as senhas e chaves criptográficas de acesso, pois elas podem ser reveladas por meio de engenharia reversa.

Detalharemos o funcionamento da criptografia em sistemas computacionais no tópico 4.7.

4.5.6 Utilizar registros de acesso (*log*) e rastreamento

No caso de um incidente relacionado com a segurança, é importante que a administração de TI reúna os detalhes relevantes para determinar o que aconteceu, e isso requer o funcionamento dos registros de acesso (*logs*). Qualquer sistema de registro deve fornecer controles para impedir a adulteração não autorizada. Os desenvolvedores devem registrar dados suficientes para rastrear e correlacionar eventos, mas não passar do limite. Um bom exemplo de “passar do limite” é registrar dados confidenciais, como *passwords* e informações de cartão de crédito. Para os casos em que o registro dessas informações seja necessário, os dados confidenciais devem ser ocultados antes de serem gravados no registro de *log*.

Exemplos de informações mínimas que devem ser registradas incluem:

- a) eventos de autenticação e autorização de acesso de usuário;
- b) nome de usuário ou endereço de e-mail;
- c) endereço da máquina do cliente (endereço IP);
- d) data e hora;
- e) código de evento (para permitir filtragem rápida);
- f) descrição do evento;
- g) resultado do evento (por exemplo, acesso de usuário permitido ou rejeitado);
- h) alterações na configuração de segurança do aplicativo.

Uma boa prática recomendada é diferenciar entre registros de monitoramento, relevantes para problemas de configuração e registros de auditoria, relevantes para análise forense para o detalhamento de problemas de segurança de aplicativos.

4.5.7 Efetuar testes para garantia da segurança da aplicação

As atividades de teste validam a implementação segura de um produto, o que reduz a probabilidade de *bugs* de segurança serem liberados e descobertos por clientes ou usuários mal-intencionados. O objetivo não é adicionar segurança por meio de testes, mas sim validar a robustez e segurança do aplicativo.

Métodos de teste automatizado são destinados a encontrar certos tipos de *bugs* de segurança, e devem ser realizados no código-fonte de todos os produtos em desenvolvimento, porque o custo de execução desses testes automatizados é relativamente baixo. Alguns passos podem ser seguidos para a realização de testes de segurança, os quais seguem descritos a seguir:

- ✖ **determinar a superfície de ataque** – deve-se ter uma compreensão atualizada e completa da superfície de ataque. Uma vez que a superfície de ataque está determinada, o teste pode então se concentrar em áreas onde os requisitos de risco ou de conformidade são os mais altos. Produtos com uma grande superfície de ataque ou processamento de entrada complexa são mais suscetíveis a ataques.
- ✖ **usar ferramentas de teste apropriadas** – diferentes ferramentas têm focos diferentes. Alguns *scanners* de vulnerabilidade de aplicativos de rede e *web* podem apontar erros de programação. Alguns desses *scanners* podem testar classes conhecidas de vulnerabilidades, como injecções SQL e vulnerabilidades de *scripts* entre sites. O uso de ferramentas automatizadas exigirá uma cuidadosa configuração e ajustes para obtenção de resultados adequados. Uma ferramenta automatizada que é executada cegamente contra um sistema sem entender o sistema ou sua superfície de ataque pode não testar algumas partes do sistema, ou testá-lo com o tipo errado de entradas.

- × **executar testes de fuzz** – teste de *fuzz* é uma técnica de teste de segurança e confiabilidade que se baseia na construção intencional de dados mal formatados, inválidos e inesperados e, em seguida, inserção destes dados no sistema para ver como ele responde. O processo de teste de *fuzz* pode ser demorado, portanto a automação é crítica. Também é importante dar prioridade aos pontos de entrada de maior exposição para o teste de *fuzz*, por exemplo, uma porta TCP não autenticada e remotamente acessível, porque os pontos de entrada de maior exposição são mais acessíveis aos atacantes. Os testes de *fuzz* podem ser usados em conjunto com outros tipos de testes, por exemplo, um *scanner* de vulnerabilidades mais focado pode ser usado para injetar entradas *fuzz* no produto de destino.

4.6 Segurança na administração, aquisição e uso de software

As organizações necessitam ter políticas claras, abrangentes e consistentes quanto à aquisição e utilização de software, de forma a prevenir o mau uso e penalidades previstas em lei. É necessário estabelecer responsáveis formais pela compra, provendo assim um meio único de entrada na organização, evitando assim a utilização de produtos não homologados. A mesma área pode ser responsável por desenvolver um procedimento de atualização de softwares, bem como efetuar o gerenciamento das licenças dos mesmos.

A organização deve manter um controle rigoroso a fim de evitar que a quantidade de softwares instalados não seja discrepante em relação à quantidade de softwares adquiridos (exceto para produtos de distribuição livre). É necessário investir em conscientização a fim de criar uma cultura de não propagação de softwares sem licença (“pirata”), pois o uso destes traz grandes riscos em termos de segurança da informação.

Ferreira (2008) lista as principais regras para aquisição, instalação e manuseio de software:

- a) compras devem ser avaliadas e aprovadas pela área de TI;
- b) aos usuários deve ser proibido a instalação direta de software, quando necessário devem ser solicitadas credenciais de administrador de rede para tal;
- c) as estações de trabalho devem possuir os softwares cuja utilização foi previamente estabelecida formalmente pela organização;
- d) os aplicativos adquiridos devem estar acompanhados de suas respectivas notas fiscais;
- e) as mídias de instalação originais devem ser armazenadas em local seguro de forma a restringir o acesso somente a pessoal autorizado;
- f) devem ser cumpridas as instruções e restrições descritas pelo contrato de licença do software.

Existem no mercado aplicativos gratuitos e também pagos que auxiliam os administradores de rede a efetuarem um inventário completo de suas estações de trabalho. O uso destas ferramentas auxilia na tarefa de efetuar a reconciliação entre a quantidade de licenças adquiridas e a quantidade de licenças em uso, visando a apuração de eventuais consistências. Manter um inventário atualizado é responsabilidade da equipe de TI da organização.

4.7 Criptografia

A criptografia tem uma longa história que remonta ao tempo em que os povos antigos, como gregos e romanos enviavam mensagens secretas embarralhando letras, de forma que fossem apenas decifráveis por uma chave secreta.

Os gregos antigos usaram uma ferramenta chamada **Cítala** (ou Bastão de Licurgo) para ajudar a criptografar suas mensagens mais rapidamente usando uma cifra de transposição. Eles enrolavam a tira de pergaminho em volta do cilindro, escreviam a mensagem e, em seguida, quando desenroladas apresentam um texto sem sentido devido ao embaralhamento das letras (vide figura a seguir).

Figura 4.3 – Instrumento antigo de criptografia (cítala)



Fonte: *Oxford Math Center*, (<http://www.oxfordmathcenter.com/drupal7/node/486>).

Este método de criptografia poderia ser facilmente quebrado, todavia é um dos primeiros exemplos de criptografia de que se tem notícias de utilização.

Júlio César usou um método semelhante durante seu tempo para se comunicar com seus generais, deslocando cada letra do alfabeto para a direita ou para a esquerda, de acordo com um número de posições. Esta é uma técnica de criptografia conhecida como “cifra de César”. Por exemplo, usando o exemplo de cifra da figura abaixo você escreveria a palavra “FAEL” como “IDHO”.

Figura 4.4 – Cifra de César

Normal : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cifrado : DEFGHIJKLMNOPQRSTUVWXYZABC

Fonte: Elaborada pelo autor.

Uma vez que apenas o destinatário da mensagem sabia a cifra, seria difícil para um terceiro decodificar a mensagem, mas a pessoa que tinha a cifra poderia facilmente decodificá-la e lê-la.

Outras criptografias simples como o **diagrama de Políbio** usam uma cifra polialfabética que traduz cada letra por meio das posições numéricas correspondentes na parte superior e lateral do diagrama (figura a seguir). Neste exemplo a palavra “FAEL” seria cifrada por meio do código “21 11 31 42”

Figura 4.5 – Diagrama de Políbio

	1	2	3	4	5
1	A	F	E	D	M
2	P	B	C	L	N
3	Q	G	J	K	O
4	R	H	I	S	T
5	W	V	U	X	Y

Fonte: Elaborada pelo autor.

Os métodos de criptografia continuaram evoluindo ao longo dos anos. Durante a Segunda Guerra Mundial, os alemães usaram a máquina **Enigma** para enviar e receber transmissões criptografadas, as quais perduraram durante anos até que matemáticos poloneses foram capazes de decifrá-la, sendo este um dos fatores importantes na vitória dos aliados.

O desenvolvimento dos computadores após a Segunda Guerra Mundial tornou possível o desenvolvimento de cifras muito mais complexas. Além disso, os computadores permitiram a criptografia de qualquer tipo de dados representável em qualquer formato binário, ao contrário de cifras clássicas que apenas criptografavam textos em linguagem escrita.

As pesquisas acadêmicas abertas em criptografia são relativamente recentes, começando somente em meados da década de 1970. O primeiro padrão mundial foi desenvolvido pela IBM, denominado *Data Encryption Standard* (DES), sendo selecionado pelo governo americano para ser utilizado em seus sistemas em 1976.

Desde então, a criptografia tornou-se uma ferramenta amplamente utilizada em comunicações, redes de computadores e segurança computacional em geral. Algumas técnicas criptográficas modernas podem manter suas chaves secretas de maneira que as funções matemáticas que as sustentam são intratáveis, de modo que há conexões profundas com a matemática abstrata.

Além de estar cientes da história e dos algoritmos criptográficos, os desenvolvedores de sistemas também devem considerar os possíveis avanços tecnológicos futuros enquanto trabalham em seus projetos. Por exemplo, as

melhorias contínuas no poder de processamento dos computadores aumentaram o alcance dos ataques de **força bruta**.

Essencialmente, antes do início do século XX, a criptografia se preocupava principalmente com padrões lexicográficos. Desde então, a ênfase mudou, e a criptografia agora faz uso extensivo da matemática, incluindo aspectos da teoria da informação, complexidade computacional, estatística, combinatória, álgebra abstrata, teoria dos números e matemática finita em geral. Vamos aprofundar nosso estudo sobre criptografia moderna nos próximos tópicos!

Saiba mais

Ataque de força bruta, ou busca exaustiva de chave, é um ataque criptoanalítico que pode, em teoria, ser usado contra quaisquer dados criptografados. Ele consiste de verificação sistemática de todas as possíveis chaves e senhas até que as corretas sejam encontradas. No pior dos casos, isto envolveria percorrer todo o espaço de busca.

4.7.1 Criptografia de chave simétrica

Para explicar esse conceito, usaremos a metáfora do serviço postal descrita na maioria das literaturas, que consiste da transmissão de uma mensagem entre os personagens fictícios Alice e Bob, a fim de facilitar a compreensão do funcionamento dos algoritmos de chave simétrica.

Alice coloca sua mensagem secreta em uma caixa, e tranca a caixa usando um cadeado, do qual ela tem a chave. Em seguida, envia a caixa para Bob por correio normal. Quando Bob recebe a caixa, ele usa uma cópia idêntica da chave de Alice (que ele de alguma forma obteve anteriormente) para abrir a caixa e ler a mensagem. Bob pode então usar o mesmo cadeado para enviar sua resposta secreta. A figura a seguir detalha este cenário:

Figura 4.6 – Transmissão de mensagem com criptografia simétrica



Fonte: Elaborada pelo autor.

Os algoritmos de chave simétrica podem ser divididos em cifras de fluxo e cifras de bloco. Cifras de fluxo criptografam os bits da mensagem um de cada vez, e os de bloco criptografam um bloco (por exemplo de 64 bits) como uma única unidade.

A principal vantagem do algoritmo simétrico é a velocidade e facilidade em criptografar e descriptografar dados, dando-lhe muito bom desempenho de leitura e escrita, exigindo pouco poder de processamento e recursos de hardware para tal.

A principal desvantagem no uso de chaves simétricas é a questão do transporte da chave. A chave secreta deve ser transmitida ao receptor antes da mensagem real ser transmitida. Como os meios de comunicação eletrônica são inseguros em sua maioria, não é possível garantir que não haverá interceptação da chave por um terceiro. Portanto, a única maneira segura de trocar chaves seria trocá-las pessoalmente. Outra desvantagem reside no fato de que como cada par necessita de uma chave específica para se comunicar, o armazenamento destas em uma rede com muitos usuários é relativamente complexo e oneroso.

Existem muitos algoritmos diferentes de criptografia simétrica atualmente. O quadro a seguir lista as principais características de cada algoritmo:

Quadro 4.2 – Algoritmos de criptografia simétrica

Algoritmo	Bits	Descrição
AES	128	O Advanced Encryption Standard (AES) é uma cifra de bloco, anunciado pelo <i>National Institute of Standards and Technology</i> (NIST) em 2003, fruto de concurso para escolha de um novo algoritmo de chave simétrica para proteger informações do governo federal, sendo adotado como padrão pelo governo dos Estados Unidos, é um dos algoritmos mais populares, desde 2006, usado para criptografia de chave simétrica, sendo considerado como o padrão substituto do DES. O AES tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits, ele é rápido tanto em software quanto em hardware, é relativamente fácil de executar e requer pouca memória.

Algoritmo	Bits	Descrição
DES	56	Originalmente desenvolvido por pesquisadores da IBM no início da década de 1970, o <i>Data Encryption Standard</i> (DES) foi o algoritmo simétrico mais utilizado no mundo até a padronização do AES. Em 1997, o NIST anunciou uma iniciativa para escolher um sucessor de DES, sendo o mesmo quebrado por “força bruta” nesta iniciativa. Em 2003 passou a recomendar a utilização do 3DES.
3DES	112 ou 168	O algoritmo 3DES é uma variação do DES, onde são executadas três iterações do algoritmo DES; uma chave criptográfica diferente pode ser usada em cada iteração. O algoritmo 3DES é mais lento que o DES simples.
IDEA	128	O IDEA (<i>International Data Encryption Algorithm</i>) é um algoritmo de criptografia desenvolvido na Suíça. Ele usa uma cifra de bloco com uma chave de 128 bits, e é considerado muito seguro. Está entre os melhores algoritmos conhecidos publicamente. Nos vários anos em que tem sido usado, nenhum ataque prático sobre ele foi publicado. O uso não-comercial de IDEA é gratuito, um dos exemplos de utilização é no PGP, programa de criptografia de e-mails conhecido mundialmente.
Blowfish	32 a 448	O algoritmo <i>Blowfish</i> usa uma chave de comprimento variável, de 32 bits a 448 bits, sendo bastante versátil quanto a seu uso. É significativamente mais rápido do que DES. Não é patenteado e está disponível gratuitamente para todos os usos.

Algoritmo	Bits	Descrição
Twofish	128	É uma das poucas cifras incluídas no OpenPGP. O Twofish é uma chave simétrica que emprega a cifra de bloco de 128 bits, utilizando chaves de tamanhos variáveis, podendo ser de 128, 192 ou 256 bits. Ele realiza 16 interações durante a criptografia, sendo um algoritmo bastante veloz. A cifra Twofish não foi patenteada estando acessível no domínio público, como resultado, o algoritmo Twofish é de uso livre para qualquer um utilizar sem restrição.
RC2	8 a 1024	Algoritmo desenvolvido por Ron Rivest em 1987. "RC" significa "Cifra de Ron" ou " <i>Rivest Cipher</i> ". Outras cifras projetadas por Rivest incluem RC4, RC5 e RC6.
CAST	128	Os detalhes iniciais do algoritmo foram mantidos em segredo – propriedade da <i>RSA Security</i> – mas em 1996, o código-fonte do RC2 foi publicado anonimamente. É um algoritmo de bloco com uma chave de tamanho variável.

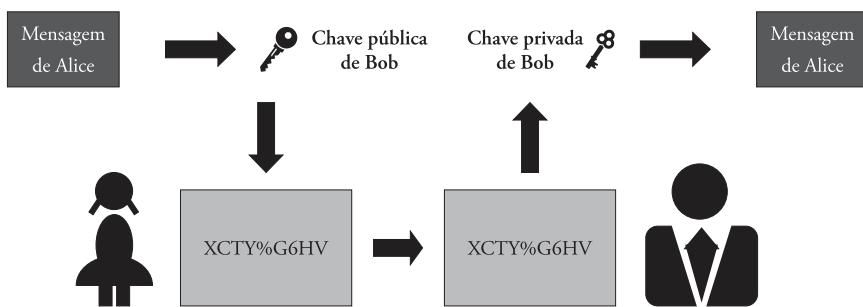
Fonte: Ronielton Rezende Oliveira (Revista Segurança Digital 2012).

4.7.2 Criptografia de chave assimétrica

Para explicar o conceito de chave assimétrica, também usaremos a metáfora do serviço postal de envio de mensagem entre os personagens Alice e Bob.

Em um sistema de chave assimétrica, Bob e Alice têm cadeados diferentes, em vez de cadeados com várias chaves iguais do exemplo simétrico. Primeiro, Alice pede a Bob para enviar seu cadeado aberto (chave pública de Bob) para ela por meio do correio normal, mantendo sua chave para si mesmo. Quando Alice recebe o cadeado, ela usa o mesmo para lacrar uma caixa contendo sua mensagem e envia a caixa lacrada para Bob. Bob pode então destravar a caixa com sua chave original (chave privada de Bob) e ler a mensagem de Alice. Para responder, Bob também deve ter em mãos o cadeado aberto de Alice para lacrar a caixa com a mensagem antes de enviá-la de volta para ela. A figura a seguir detalha este conceito:

Figura 4.7 – Transmissão de mensagem com criptografia assimétrica



Fonte: Elaborada pelo autor.

A vantagem crítica de um sistema de criptografia assimétrica é que Bob e Alice nunca precisam enviar uma cópia de suas chaves privadas um para

o outro. Isso impede que um terceiro (talvez, no exemplo, um funcionário corrupto do serviço postal) copie uma chave enquanto está em trânsito, permitindo que o terceiro espie todas as futuras mensagens enviadas entre Alice e Bob. Além disso, se Bob fosse descuidado e permitisse que alguém copiasse sua chave, as mensagens de Alice para Bob ficariam comprometidas, mas as mensagens de Alice para outras pessoas permaneceriam secretas, já que as outras pessoas estariam fornecendo cadeados diferentes para Alice usar.

A criptografia assimétrica usa chaves diferentes para criptografia e descriptografia. O destinatário da mensagem possui uma chave privada e uma chave pública. A chave pública é distribuída entre os remetentes da mensagem e eles usam a chave pública para criptografar a mensagem. O destinatário usa sua chave privada para descriptografar qualquer mensagem que tenha sido criptografada usando a sua chave pública.

Há uma grande vantagem em utilizar esta forma de criptografia em comparação com a criptografia simétrica. Não é preciso enviar algo secreto (como nossa chave de criptografia simétrica ou senha) por meio de um canal inseguro. Sua chave pública fica acessível a quem interessar, ela não é secreta e não deve ser. Sua chave privada ficará armazenada de forma segura em seu dispositivo pessoal.

A desvantagem deste sistema assimétrico é a complexidade empregada no desenvolvimento dos algoritmos que devem ser capazes de reconhecer o par de chaves existentes, bem como poder relacionar as mesmas chaves no momento oportuno, o que acarreta em grande demanda de processamento computacional, podendo tornar o processo mais lento dependendo do hardware utilizado.

Assim como existem diversos algoritmos de criptografia simétrica, também existe variedade de algoritmos assimétricos. O quadro 4.3 lista as principais características de cada algoritmo:

Quadro 4.3 – Algoritmos de criptografia assimétricos

Algoritmo	Descrição
RSA	<p>O algoritmo RSA foi descrito pela primeira vez em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman do MIT. No algoritmo RSA, tanto a chave pública como a privada podem criptografar uma mensagem. A chave oposta à usada para criptografar uma mensagem é usada para descriptografar. Este atributo é uma das razões pelas quais a RSA se tornou o algoritmo assimétrico mais utilizado atualmente. A segurança do RSA baseia-se na dificuldade de fatoração de grandes números inteiros que são o produto de dois grandes números primos. A multiplicação destes dois números é fácil, mas a determinação dos números primos originais é considerada inviável devido ao tempo que demoraria mesmo usando os supercomputadores atuais. A força de criptografia está diretamente ligada ao tamanho da chave criptográfica. As chaves RSA normalmente têm 1024 ou 2048 bits. No Brasil, o RSA é utilizado pela ICP-Brasil, no seu sistema de emissão de certificados digitais, e a partir do dia 1º de janeiro de 2012, as chaves utilizadas pelas autoridades certificadoras do país, passam a serem emitidas com o comprimento de 4.096 bits, em vez dos 2.048 bits anteriores.</p>
ElGamal	<p>O algoritmo ElGamal fornece uma alternativa para o RSA para uso em criptografia de chave pública. A segurança do algoritmo ElGamal depende da dificuldade denominada problema do logaritmo discreto, ou seja, da dificuldade de calcular logaritmos discretos em um corpo finito.</p> <p>A criptografia ElGamal é probabilística, o que significa que um único texto não criptografado pode ser criptografado em muitos textos possíveis.</p>

Algoritmo	Descrição
Diffie-Hellman	O algoritmo Diffie-Hellman foi desenvolvido por Whitfield Diffie e Martin Hellman em 1976. O objetivo principal do algoritmo não é criptografar os dados, mas sim gerar a mesma chave criptográfica privada em ambas as extremidades, de modo que não há necessidade de transferir esta chave de um ponto de comunicação para outro. A limitação mais séria do Diffie-Hellman é a falta de autenticação. As comunicações usando Diffie-Hellman por si só são vulneráveis à interceptação.
Curvas Elípticas	Criptografia de curva elíptica (ECC) é um algoritmo baseado na teoria de curva elíptica que pode ser usado para criar chaves criptográficas mais rápidas, menores e mais eficientes. O ECC gera chaves por meio das propriedades da equação da curva elíptica em vez do método tradicional de geração como o produto de números primos muito grandes. Como o ECC ajuda a estabelecer uma segurança equivalente aos algoritmos tradicionais, com menor poder de computação e uso de recursos da bateria, está se tornando amplamente utilizado em aplicativos móveis.

Fonte: Elaborada pelo autor.

Saiba mais

Por muitos anos, o protocolo SSL (*Secure Sockets Layer*) tem protegido as transações da web usando criptografia entre o navegador cliente e o servidor web, protegendo o usuário de qualquer ataque de espião do meio de transmissão (por exemplo, *sniffing de rede*).

4.8 Certificado digital

O equivalente digital de um documento de identificação, utilizado em conjunto com um sistema de criptografia de chave pública, é denominado Certificado Digital. O certificado digital contém, além da chave pública, informações sobre seu proprietário, como nome, endereço e outros dados pessoais. Para garantia das informações, o certificado é assinado por alguém em quem o proprietário deposita sua confiança, ou seja, uma autoridade certificadora (*Certification Authority – CA*), funcionando como uma espécie de “cartório virtual”.

No Brasil, o órgão da autoridade certificadora raiz é o ICP-Brasil. A Infraestrutura de Chaves Públicas Brasileira é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Existem também as autoridades certificadores abaixo do ICP-Brasil, entre elas: Serpro (AC-SERPRO), Caixa Econômica Federal (AC-CAIXA), Serasa Experian (AC-SERASA), Receita Federal do Brasil (AC-RFB), Certsign (AC-Certisign), Imprensa Oficial do Estado de São Paulo (AC-IOSP), entre outras.

O Instituto Nacional de Tecnologia da Informação define o ICP-Brasil como “um conjunto de técnicas, práticas e procedimentos que foram traçadas pelo seu Comitê Gestor com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública”. É composto por uma cadeia de autoridades certificadoras, formada por uma Autoridade Certificadora Raiz (AC-Raiz), Autoridades Certificadoras (AC) e Autoridades de Registro (AR) e, ainda, por uma autoridade gestora de políticas, ou seja, o Comitê Gestor da ICP-Brasil. Estes órgãos gerenciam todas as emissões e revogações de Certificados Digitais no Brasil.

Saiba mais

Você pode consultar na internet todas as informações sobre a Infraestrutura de Chaves Públicas Brasileira, no endereço oficial do Governo Federal: <<http://www.iti.gov.br/icp-brasil>>.

4.9 Assinatura digital

As assinaturas digitais são como “impressões digitais” eletrônicas. Na forma de uma mensagem codificada, a assinatura digital associa de

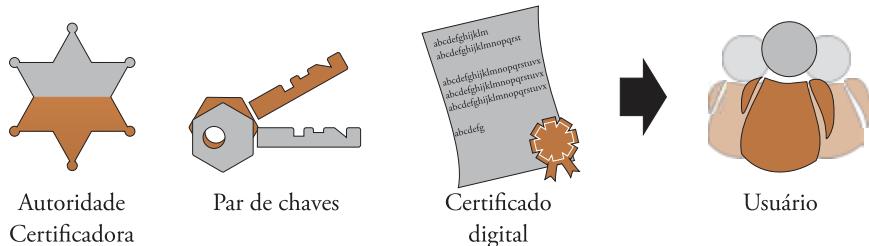
forma segura um assinante a um documento em uma transação eletrônica. As assinaturas digitais usam um formato padrão aceito mundialmente, denominado *Public Key Infrastructure* (PKI), ou Infraestrutura de Chaves Públicas, para fornecer os mais altos níveis de segurança e aceitação universal.

A PKI é um sistema criptográfico assimétrico que usa duas chaves: uma chave pública conhecida por todos e uma chave privada. A chave privada fica em posse do proprietário (em um dispositivo como *token* ou *smartcard*) e deve ser mantida em ambiente seguro. A característica principal deste sistema é que as chaves públicas e privadas estão relacionadas de tal forma que somente a chave pública pode ser usada para criptografar mensagens e somente a chave privada correspondente pode ser usada para descriptografá-las. Além disso, é praticamente impossível deduzir a chave privada se alguém souber a chave pública de uma pessoa.

4.9.1 Geração do par de chaves

Para assinar digitalmente documentos, um usuário precisa obter um par de chaves: chave pública e chave privada. Como estudamos no tópico sobre Certificados Digitais, este processo só poderá ser realizado pelas Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e demais prestadores de serviço habilitados na ICP-Brasil. A chave privada não é compartilhada e é usada apenas por documentos assinados pelo usuário. A chave pública estará disponível para todos, sendo usada para validar a assinatura digital do signatário. A figura 4.8 exemplifica este processo:

Figura 4.8 – Geração do par de chaves



Fonte: Elaborada pelo autor.

4.9.2 Assinando digitalmente um documento

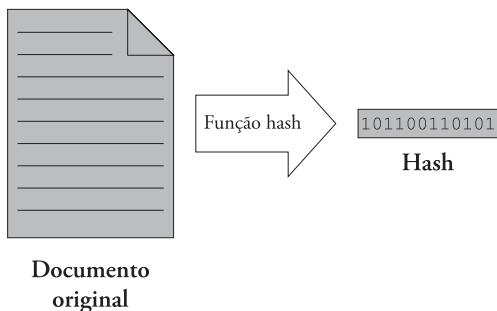
Para criar uma assinatura digital, o software de assinatura cria uma função *hash* unidirecional dos dados eletrônicos a serem assinados. A chave privada é então usada para criptografar o *hash*. O *hash* criptografado é a assinatura digital. A razão para criptografar o *hash* em vez de toda a mensagem ou documento é que uma função de *hash* pode converter uma entrada arbitrária em um valor de comprimento fixo, que normalmente é muito menor. Isso economiza tempo e recurso computacional.

A assinatura também é marcada com a data e hora em que o documento foi assinado. Se o documento for alterado após a assinatura, a função *hashing* mudará de valor, e consequentemente a assinatura digital será invalidada.

O receptor do documento utiliza a chave pública do emissor para descriptografar a assinatura. Se a chave pública não puder descriptografar a assinatura (por meio da comparação dos *hashes*), isso significa que a assinatura não poderá ser validada. Iremos detalhar melhor este processo nas etapas de “a” a “e” a seguir:

- a) quando o emissor clica em “assinar digitalmente” no software compatível com assinatura digital de documentos, a função *hash* gera um valor único, utilizando um algoritmo matemático. Este *hash* é específico para este documento em particular. Mesmo a menor alteração (em apenas um bit) resultaria em um *hash* completamente diferente, vide figura a seguir:

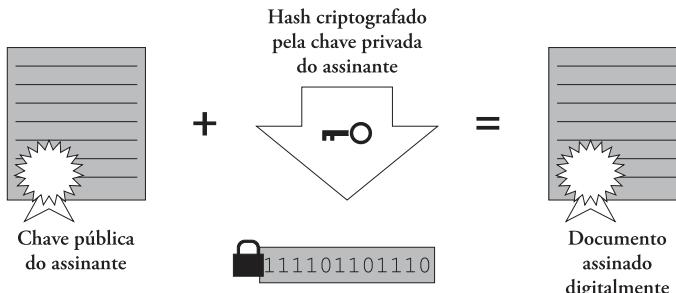
Figura 4.9 – Função *hash*



Fonte: Elaborada pelo autor.

O *hash* é criptografado usando a chave privada do signatário. O *hash* criptografado e a chave pública do assinante são combinados em uma assinatura digital, que é anexada ao documento, vide figura a seguir:

Figura 4.10 – Criptografia do *hash*



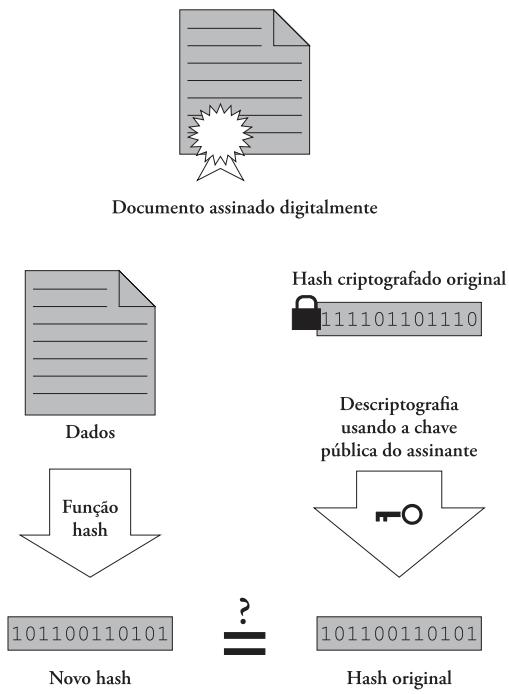
Fonte: Elaborada pelo autor.

O documento assinado digitalmente está pronto para distribuição.

Quando o receptor abre o documento em um programa compatível com verificação de assinatura digital, o programa usa automaticamente a chave pública do assinante (que foi incluída na assinatura digital com o documento) para descriptografar o *hash* do documento.

O programa calcula um novo *hash* para o documento. Se este novo *hash* corresponder ao *hash* descriptografado da etapa “d” acima, o programa sabe que o documento não foi alterado e exibe uma mensagem de validação do tipo: “O documento não foi modificado desde que esta assinatura foi

Figura 4.11 – Validação da assinatura digital



Fonte: Elaborada pelo autor.

“aplicada”. O programa também valida a chave pública usada na assinatura pertence ao signatário e exibe o nome do assinante ao leitor. As etapas “d” e “e” são exemplificadas na figura a seguir:

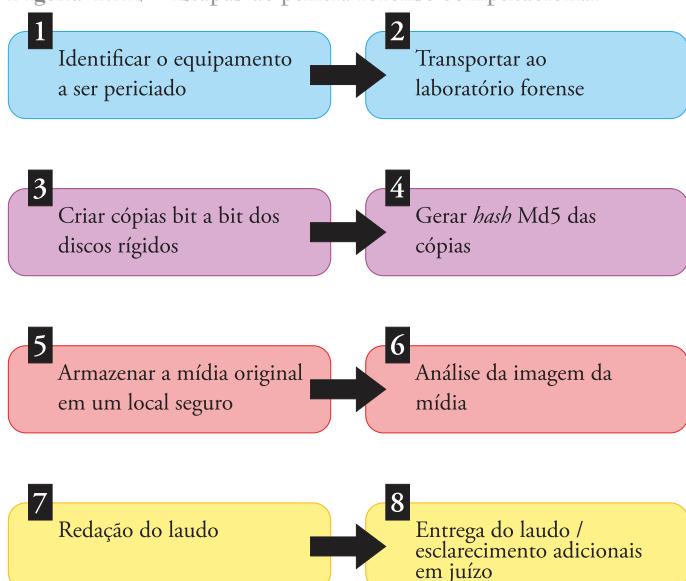
4.10 Forense computacional

Quando ocorre um incidente de segurança em uma empresa, por vezes será necessário observar procedimentos de preservação de evidências, com o objetivo de não prejudicar ações futuras que envolvam investigação interna ou externa, incluindo ações policiais e judiciais.

As ciências forenses tratam da aplicação de princípios das ciências físicas ao direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade. A área de forense computacional consiste no uso de métodos científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital com validade probatória em juízo.

A forense computacional poderá ser utilizada em situações como quebra de contrato (podendo ser entre funcionário e empresa ou entre empresas), quando houver roubo ou divulgação de informações sigilosas, disputa entre empregados entre

Figura 4.12 – Etapas de perícia forense computacional



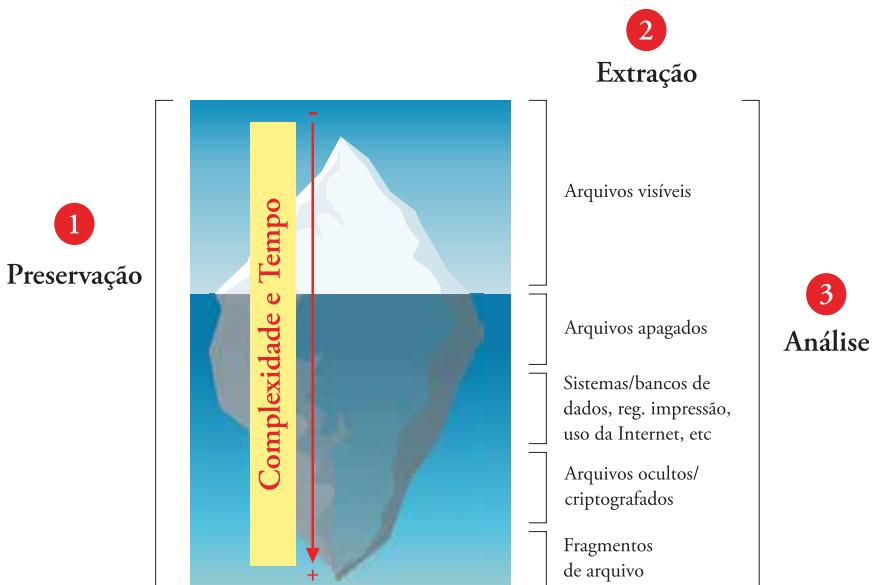
Fonte: Elaborada pelo autor.

outros fatores. É necessário também efetuar a coleta de evidências utilizando-se de metodologias forenses para proteger a organização de incidentes similares no futuro e também para fundamentar corretamente possíveis ações cíveis ou criminais no âmbito jurídico.

A aplicação de metodologias forenses normalmente necessita do auxílio de peritos especialistas nesta área, que atuam no mercado de perícia digital. Existem basicamente oito etapas durante um processo de perícia forense computacional, desde a identificação do equipamento até a entrega do laudo por parte do perito. Tais etapas são detalhadas na figura 4.12:

Os dados armazenados em um computador são como um *iceberg*. Quanto mais o perito necessitar aprofundar-se em um exame, como por exemplo, para obter informações a partir de fragmentos de arquivos, mais tempo será necessário dispender para executar a tarefa de produzir evidências de um incidente. Vide figura a seguir:

Figura 4.13 – Complexidade de exame forense computacional



Fonte: Elaborada pelo autor.

Saiba mais

Para fins de observação de todas as etapas correspondentes a um exame forense computacional recomenda-se a leitura da norma ISO/IEC 27037. Esta norma fornece diretrizes para atividades específicas no manuseio de evidências digitais como a identificação, coleta, aquisição e preservação de evidência digital que possam possuir valor probatório.

Síntese

Neste capítulo estudamos aspectos tecnológicos fundamentais relacionados à segurança da informação. Os conceitos de softwares malicioso, bem como os diferentes tipos destes exigem estratégias de combate específicas para cada tipo.

Evidente também é o cuidado que o desenvolvedor de software necessitar ter para o desenvolvimento seguro de aplicações.

Por fim conceitos que envolvem a criptografia e assinaturas digitais são indispensáveis ao conhecimento de soluções que visam garantir os aspectos fundamentais da segurança da informação na tramitação e guarda de documentos.

Atividades

1. Qual a diferença principal entre *vírus* e *worm*?
2. De que forma evitar a concatenação de *strings* SQL para cláusulas de SQL dinâmicas contribui para o desenvolvimento de aplicativos seguros?
3. Quanto aos conceitos básicos de Segurança da Informação é correto afirmar que a criptografia simétrica (Questão Concurso Público ESAF 2006 – Prova 1 – Cargo Administrador):
 - a) usa um algoritmo de criptografia que requer que a mesma chave secreta seja usada na criptografia e na descriptografia.

- b) é um método de criptografia no qual duas chaves diferentes são usadas: uma chave pública para criptografar dados e uma chave particular para descriptografá-los.
- c) é um método de criptografia no qual duas chaves diferentes são usadas: uma chave particular para criptografar dados e uma chave pública para descriptografá-los.
- d) é o processo de regravação de partes de um arquivo em setores contíguos de um disco rígido a fim de aumentar a segurança da informação.
- e) é o resultado de tamanho fixo, também chamado de síntese da mensagem, obtido pela aplicação de uma função matemática unidirecional a uma quantidade de dados arbitrária.

4. A respeito de segurança da informação:

A assinatura digital é um código criado mediante a utilização de uma chave privada, que permite identificar a identidade do remetente de dada mensagem. (Questão Concurso Público TELEBRÁS 2015 – Cargo Especialista em Gestão de Telecomunicações)

- a) Certo
- b) Errado

5

Aspectos Humanos da Segurança da Informação

Após o ESTUDO dos aspectos tecnológicos que envolvem a segurança da informação passaremos a estudar os aspectos humanos, ou seja, o papel de cada ator participante do processo de segurança da informação. Visto que a segurança tem início e término nas pessoas, é fundamental compreender as técnicas utilizadas por aqueles que desejam burlar políticas de segurança da informação a fim de obter acesso a informações privilegiadas. Para tanto, estudaremos as técnicas de engenharia social ensinado também estratégias de proteção contra estas técnicas.

DISCUTIREMOS TAMBÉM SOBRE os procedimentos em casos de violações, baseando-se na legislação penal vigente hoje no Brasil e finalizaremos com o estudo sobre os papéis desempenhados pelos profissionais da segurança da informação.

Objetivo da aprendizagem:

- × Compreender o papel dos atores participantes do processo de segurança da informação.

5.1 Engenharia social

A definição de engenharia social é muito mais abrangente do que apenas dentro do contexto da segurança da informação. Ela é usada, por exemplo, durante a infância, por meio da forma como as crianças conseguem que seus pais cedam às suas demandas. Também é usada na forma como os professores interagem com seus alunos, ou como médicos, advogados e psicólogos obtêm informações de seus pacientes ou clientes. Neste contexto amplo a engenharia social é o ato de manipular uma pessoa para efetuar uma ação que pode ou não estar no melhor interesse desta. Como exemplo, podemos citar o psicólogo, que por meio de uma série de perguntas bem concebidas pode ajudar um paciente a chegar à conclusão de que uma mudança é necessária em algum aspecto da vida.

Embora qualquer pessoa possa aprender tais técnicas de manipulação social, algumas aparentam ter um “talento nato” para isto. É o caso de um dos mais famosos *hackers* da história: Kevin Mitnik. De nacionalidade norte americana, ele iniciou sua vida de trapaças ainda na adolescência, comprometendo redes telefônicas, corporações e a segurança de importantes departamentos do governo americano. Após sua prisão e cumprimento de pena, abriu uma empresa de proteção a informações pessoais, e passou a dar palestras, sendo uma referência na área de segurança da informação.

No contexto da segurança da informação, podemos conceituar engenharia social como o “método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações” (CERT.br, 2016).

Muitas pessoas, ao longo de várias décadas, usaram a engenharia social como um método para pesquisar e coletar dados. Esses primeiros engenheiros sociais usavam a informação obtida como uma forma de chantagem contra outras organizações. A engenharia social tem sido usada desde o início

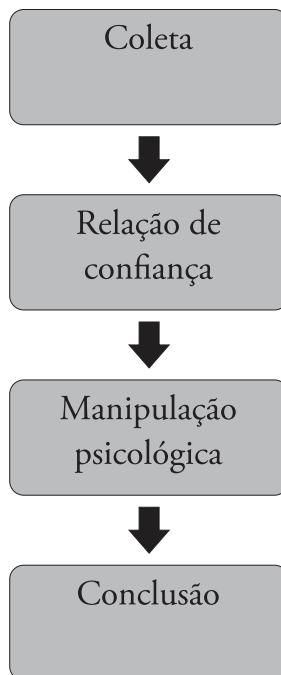
da informatização para obter acesso não autorizado a várias organizações, de pequeno a grande porte. Um *hacker* que passa várias horas tentando quebrar senhas pode economizar muito tempo ligando para um funcionário da organização, fazendo-se passar como um atendente de suporte ou um funcionário de TI, apenas convencendo o usuário a dar a senha para ele.

5.1.1 O ciclo de vida da engenharia social

Cada ataque de engenharia social é único, mas de modo geral podemos elaborar um ciclo de vida aproximado de todas as atividades que um ataque bem-sucedido de engenharia social apresenta.

A figura a seguir mostra uma representação geral do ciclo de vida da engenharia Social em quatro etapas principais:

Figura 5.1 - Ciclo de vida da engenharia social



Fonte: Elaborada pelo autor.

- × **Coleta** é a etapa de levantamento de informações sobre o(s) alvo(s) e o ambiente circunvizinho a este. Esta etapa pode revelar os indivíduos relacionados com o alvo, com os quais o atacante poderá estabelecer um relacionamento, de modo a melhorar as chances de um ataque bem-sucedido. A coleta de informações durante esta fase inclui, mas não se limita a: lista de nomes de funcionários e números de telefone; organograma; informações do departamento; informações de localização. A coleta geralmente se refere a uma das fases de pré-ataque, na qual tarefas são realizadas antes de se fazer o ataque de engenharia social real.
- × **Relação de confiança** é a fase na qual o atacante passa a desenvolver um relacionamento com o alvo, uma vez que estes possíveis alvos foram enumerados. Geralmente trata-se de um funcionário ou alguém que trabalha indiretamente no negócio de interesse do atacante. A confiança que o engenheiro social procura ganhar nesta fase será usada mais tarde para obter acesso a informações confidenciais que podem causar graves danos para a organização.
- × **Manipulação psicológica** é quando o engenheiro social utiliza a confiança que ele ganhou na fase anterior de modo a extraír a informação confidencial desejada. Uma vez que todas as informações sensíveis necessárias foram coletadas, o engenheiro social pode passar para o próximo alvo ou avançar na exploração do sistema ou processo em questão.
- × **Conclusão** é a etapa final. Depois de toda a informação desejada ter sido extraída, o engenheiro social necessita fazer uma saída discreta, de modo a não levantar qualquer tipo de suspeita desnecessária para si mesmo. Ele certifica-se de não deixar qualquer tipo de vestígio de sua atuação, de modo que pudesse levar um investigador a um rastreamento até sua verdadeira identidade.

5.1.2 Traços comportamentais humanos passíveis de exploração

Cada ataque de engenharia social procura explorar diferentes traços comportamentais específicos das vítimas, de modo que possam extraír o

máximo de informações possíveis. Exemplificamos a seguir sete traços comportamentais passíveis de exploração, embora os ataques não se limitem a explorar somente estas características.

- a) **Empolgação com uma conquista:** o cenário a seguir demonstra este comportamento. O “senhor Fulano” recebe um e-mail com o seguinte texto: “você ganhou um automóvel zero km na promoção das lojas AAA. Para receber o seu prêmio, preencha o documento anexado e envie-o para o endereço de e-mail: promocao@loja-saaa.com.br. Obs.: será necessário desabilitar seu antivírus, pois o mesmo pode bloquear o *download* do anexo, devido à assinatura digital criptografada do documento”. Esta mensagem pode parecer bastante suspeita para alguns, mas digamos que o Sr. Fulano esteve, coincidentemente, nas lojas AAA naquela semana e preencheu um cupom para participar de uma promoção. Devido à empolgação de receber uma conquista como esta, o usuário pode ser induzido ao descuido de baixar um *malware* em sua máquina que irá permitir que o remetente do e-mail possa obter acesso remoto à esta máquina.
- b) **Temor da autoridade:** muitas pessoas ficam apreensivas na presença de uma figura de autoridade, sentindo-se, de certa forma inibidas e intimidadas. Os atacantes podem assumir papéis de figuras de autoridade, como agentes da lei ou funcionários de alto escalão da empresa, para extrair informações organizacionais sensíveis das vítimas.
- c) **Desejo de ser útil:** as empresas treinam seus funcionários para serem úteis, mas raramente treinam eles para fazer parte do processo de segurança. Atacantes mal-intencionados podem usar a conexão social entre as pessoas, e o desejo delas em serem úteis, para obter informações privilegiadas. Funcionários bem-intencionados em resolver demandas de outras pessoas podem acabar dando uma grande quantidade de informações privilegiadas, que de outra forma não deveriam ser divulgadas a um estranho.
- d) **Medo de perder algo valioso:** um dos exemplos mais evidentes da exploração deste comportamento é o famoso golpe do “bilhete premiado”, no qual um golpista convence uma vítima de que possui

um bilhete premiado de loteria, fazendo com que a vítima deposite ou lhe dê em mãos um valor menor do que o prêmio do bilhete. Por vezes, utiliza-se da ajuda de um segundo golpista, que ameaça comprar o bilhete antes da vítima, evocando este sentimento na mesma do medo de perder algo valioso.

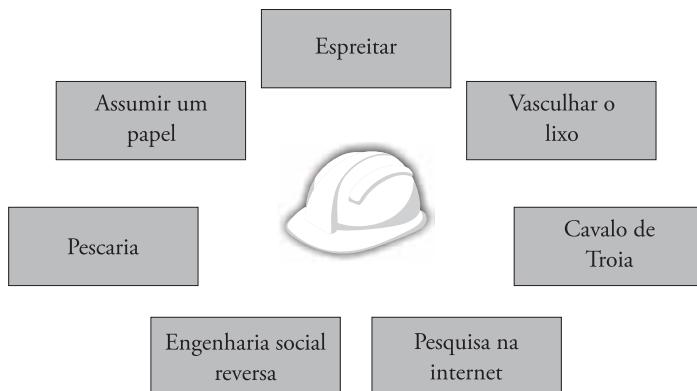
- e) **Conhecimento insuficiente:** o conhecimento sobre o sistema alvo é um dos fatores chave que diferenciam o atacante de outros funcionários da organização. Muitas vezes, devido à falta de treinamento adequado, os funcionários não possuem conhecimento completo sobre o processo ou produto e engenheiros sociais tiram proveito destas situações, criando um senso de urgência e não permitindo que o empregado tenha muito tempo para pensar e entender o fato de que está sob ataque.

5.1.3 Técnicas de engenharia social

A maneira mais fácil de entrar em um sistema computacional é simplesmente pedir permissão a quem utiliza o mesmo. Afinal, não importa quanta criptografia e tecnologia de segurança o administrador tenha implementado, uma rede nunca é completamente segura. Os administradores não podem se livrar do elo mais fraco: o fator humano. Não importa quantos *firewalls*, redes privadas virtuais (VPNs) ou dispositivos de criptografia existem em uma organização, se os seus funcionários estiverem dispostos a dar acesso aos sistemas a qualquer pessoa que o solicite.

A engenharia social é mais do que ser apenas um enganador, trata-se de ser um engenheiro que descobre maneiras de manipular as pessoas para obter vantagem sobre elas. Engenheiros sociais usam muitas técnicas para atingir seus objetivos. Apenas para fins didáticos separamos algumas técnicas em categorias, embora tais classificações possam variar de acordo com a literatura pesquisada. A figura 5.2 apresenta as referidas técnicas.

Figura 5.2 - Técnicas de engenharia social



Fonte: Elaborada pelo autor.

- a) **Espreitar** (*shoulder surfing*): ocorre quando um atacante usa técnicas de observação, como olhar sobre o ombro de alguém, para obter informações enquanto a vítima está executando alguma ação que envolve o uso explícito de informações sensíveis e visíveis. A técnica é especialmente eficaz em locais lotados onde uma pessoa usa um computador, *smartphone* ou terminal bancário. Se o ato de espreitar ocorrer quando houver poucas pessoas no ambiente, o mesmo pode tornar-se rapidamente suspeito. Para minimizar o risco podem ser usados binóculos, câmeras de vigilância e outros dispositivos, dependendo da localização e situação. Algumas formas de proteção ao entrar em sistemas ou acessar dados pessoais em um dispositivo eletrônico incluem:
- I. procurar uma área onde as costas fiquem contra uma parede.
 - II. utilizar um filtro de tela ou protetor para obscurecer a visibilidade da tela.

III. localizar um local seguro longe de multidões para efetuar *login* em sistemas.

IV. tanto quanto possível, não abrir contas pessoais em público.

- b) Vasculhar o lixo (*dumpster diving*):** muitas vezes, grandes organizações jogam no lixo itens contendo informações sensíveis, como: catálogos de telefones da empresa; manuais de sistema; organogramas; manuais de política da empresa, calendários de reuniões, eventos e férias; impressões de dados sensíveis com *logins*, nomes ou senhas, impressões de código-fonte; discos e fitas; formulários de memorando; hardware desatualizado; O atacante pode usar esses itens para obter uma quantidade enorme de informações sobre a organização da empresa e estrutura de rede. Portanto, é o método de busca pelo ato de vasculhar o lixo, procurando informações potencialmente úteis rejeitadas pelos funcionários de uma empresa.
- c) Cavalo de Troia (*trojan horse*):** é um dos métodos mais utilizados atualmente por *hackers* que procuram enganar as vítimas, induzindo-as a baixar um arquivo contendo software malicioso. Detalhamos o funcionamento desta técnica no capítulo anterior, seção 4.1.
- d) Pesquisa na internet (*surfing websites*):** uma enorme quantidade de informação sobre a estrutura das organizações encontra-se disponível para todos na internet. Por vezes endereços de e-mail, números de telefone e outras informações internas estão disponíveis abertamente no site da empresa e outros fóruns. Essas informações podem ser usadas pelo atacante para refinar sua abordagem, auxiliando-o a criar um plano mais eficiente sobre o método de ataque que será utilizado. Umas das técnicas, por exemplo, é vasculhar bancos de dados de empresas de recrutamento e seleção, em busca de vagas de emprego para administradores de TI da organização a ser atacada. Uma lista de habilidades desejadas pela empresa para o cargo de administrador de rede informa ao atacante muito sobre o ambiente de rede da empresa (tecnologias que utiliza, plataformas, servidores etc.).
- e) Engenharia social reversa (*reverse social engineering*):** é um ataque no qual um invasor convence o alvo de que ele tem um problema ou pode ter um certo problema no futuro e que o atacante

está pronto para ajudar a resolvê-lo. A engenharia social reversa envolve três etapas:

- I. *sabotagem* – depois que o atacante ganha um acesso simples ao sistema, ele corrompe o mesmo ou lhe dá a aparência de estar corrompido. Quando o usuário vê o sistema no estado corrompido, ele começa a procurar ajuda para resolver o problema;
 - II. *marketing* – a fim de certificar-se de que o usuário com problemas irá se aproximar do atacante, o mesmo se anuncia como a única pessoa que pode resolver o problema enfrentado pelo usuário;
 - III. *suporte* – nesta etapa, o atacante ganha a confiança do alvo e obtém acesso a informações confidenciais, fazendo-se passar como técnico de suporte do sistema.
- f) **Pescaria (*phishing*)**: é uma forma de fraude na qual o invasor tenta capturar informações sensíveis como credenciais de *login* ou informações da conta do usuário, fazendo-se passar como uma entidade ou pessoa respeitável. Normalmente, a vítima recebe uma mensagem que parece ter sido enviada por um contato ou organização conhecidos. Um anexo ou *link* na mensagem pode instalar um *malware* no dispositivo do usuário ou direcioná-lo para um site mal-intencionado, especialmente desenvolvido para enganá-lo. O *phishing* é popular entre os criminosos virtuais, já que é muito mais fácil enganar alguém, induzindo-o a clicar em um *link* malicioso do que tentar quebrar as defesas de um computador ou sistema. Embora alguns e-mails de *phishing* sejam mal escritos e claramente identificáveis como falsos, alguns criminosos virtuais sofisticados empregam técnicas de marketing profissional, capturando a atenção de usuários vulneráveis. Campanhas de *phishing* são muitas vezes construídas em torno de grandes eventos que acontecem no ano, ou tirando proveito de notícias de última hora, como tragédias ou outras de grande repercussão nacional. Por exemplo, em época de liberação de restituição de imposto de renda pela Receita Federal, o usuário recebe uma mensagem contendo um link “clique aqui para consultar sua restituição”.

- g) **Assumir um papel (*role playing*)**: é uma das principais armas de um engenheiro social. O atacante assume um papel que inspira confiança ao usuário. Ele tenta persuadir ou reunir informações por meio do uso de uma sessão de bate-papo on-line, e-mails, telefone ou qualquer outro método que a empresa usa para interagir com o público em geral, fingindo ser um funcionário de suporte, empregado, técnico ou um ator importante na organização.

5.1.4 Estratégias de defesa contra a engenharia social

Como não existe *hardware* nem *software* específico disponível para proteger uma empresa contra a engenharia social é essencial que sejam implementadas boas práticas de segurança que auxiliem na proteção da empresa. Um dos principais pontos a ser observado é o controle de acesso físico às dependências da organização. Deve-se garantir que apenas pessoas autorizadas tenham acesso às dependências físicas desta. Todos os visitantes precisam ser acompanhados quando adentram ao ambiente da organização.

A seguir citamos outras práticas que podem auxiliar na proteção da organização:

- a) **exigir que qualquer prestador de serviço seja cadastrado e identificado apropriadamente** – via de regra, os funcionários de uma organização não são treinados a desafiar estranhos, portanto tais funcionários, especialmente da recepção devem ser treinados adequadamente, sendo orientados a solicitar assistência de superiores em casos que exijam mais cuidados.
- b) **estabelecer um padrão para que as senhas nunca sejam pronunciadas por telefone** – para situações em que seja necessário contato com o suporte para ter uma senha redefinida, a organização deve estabelecer um conjunto de palavras conhecidas apenas pelo usuário. O suporte pode então redefinir a senha para uma dessas palavras.
- c) **conscientização acerca da guarda segura de senhas** – atualmente, devido à quantidade de serviços on-line que utilizamos, estima-se que necessitamos guardar quase dez senhas de diversos serviços. Como proibir um funcionário de anotar uma senha é uma política

difícil de cumprir, o ideal é orientar acerca da guarda segura destas senhas que necessitam ser anotadas.

- d) **implementar tecnologias de identificação de chamadas de/ou para o suporte** – existem formas de configurar tons de toque diferentes para chamadas originadas internamente e chamadas originadas externamente, de forma que o funcionário possa identificar facilmente a diferença entre elas.
- e) **investir em equipamento triturador** – o ideal é que cada área ou setor de uma organização possua um equipamento triturador, de acordo com o volume de informações confidenciais que a área ou setor manipula.

As políticas, procedimentos e padrões de segurança são parte fundamental em uma estratégia organizacional contra os ataques de engenharia social. As políticas não devem conter normas ou diretrizes que possam não ser atingidas. Ao criar padrões, o administrador deve interagir com a comunidade de usuários para estabelecer o que pode ser realizado imediatamente. Devem também ser breves e concisas, para que não haja desinteresse generalizado dos funcionários em conhecê-las. Também devem ser revistas regularmente, sendo mantidas atualizadas e divulgadas através de meios internos de comunicação, como páginas de intranet, por exemplo.

Existem também sinais típicos de que um indivíduo está tentando realizar um ataque de engenharia social. Esses sinais podem incluir comportamentos como:

- ✗ recusa de fornecimento de informações de contato, quando solicitado;
- ✗ tentativa de apressar o processo de liberação de acesso;
- ✗ *name-dropping* – o ato de alguém falar sobre pessoas famosas que conheceu, muitas vezes fingindo que as conhece melhor do que realmente conhece, a fim aparentar ser mais importante e especial;
- ✗ intimidação;
- ✗ pequenos erros sobre o conhecimento do negócio;
- ✗ solicitação de informações ou acessos proibidos;

Saiba mais

Todas essas recomendações são integráveis com a construção de um plano de resposta a incidentes para neutralizar ataques de engenharia social. Lembre-se destes verbos: *preparar, detectar, analisar, conter, erradicar, recuperar e aprender*. Com isso em mente, o administrador de segurança deve perguntar a si mesmo: a equipe de resposta a incidentes está pronta para o próximo ataque de engenharia social?

5.2 Procedimentos em casos de violações

Embora políticas de segurança da informação sejam fundamentais para proteger a confidencialidade, integridade e disponibilidade das informações, nem sempre serão suficientes para impedir que violações ocorram no ambiente de uma organização. Existem usuários, por exemplo, que “empresam” sua senha a terceiros, sem preocupar-se com os danos que esta prática pode causar.

Portanto, devem ser consideradas as penalidades e processos disciplinares em casos de violação por parte de colaboradores de uma empresa. A alta administração deve deixar claro que existirão punições aos funcionários, estagiários e prestadores de serviço que desrespeitarem as normas internas que garantem a segurança da informação. A severidade da punição deverá ser proporcional ao grau de problemas e prejuízos causados à organização. Tais punições podem variar de simples advertências, até mudança de atribuições ou demissão em casos mais críticos.

O principal objetivo de estabelecer punições pelo desrespeito às normas de segurança da informação é incentivar que todos possam aderir a estas normas, bem como dar respaldo jurídico à organização em casos mais graves de violação.

Qualquer incidente envolvendo segurança da informação deve ser imediatamente reportado à alta administração da organização, bem como aos responsáveis diretos pela área de segurança, a fim de assegurar que o problema de violação foi resolvido e foram executadas ações necessárias para evitar reincidências.

Quando for detectada uma violação também é necessário averiguar as causas, consequências e circunstâncias em que ocorreu. É importante identificar se foi causada por simples desconhecimento das normas, bem como negligencia ou até mesmo ação fraudulenta.

Ferreira (2008) exemplifica algumas das infrações que são puníveis pelos termos da lei. O quadro 5.1 a seguir apresenta alguns destes exemplos.

Quadro 5.1 - Infrações puníveis pelos termos da lei

Exemplo de infração	Tipo de crime	Enquadramento jurídico
Encaminhar para várias pessoas mensagem contendo boato eletrônico	Difamação	Artigo 139 do Código Penal
Acessar um sistema com a senha de terceiros sem autorização expressa	Invasão de dispositivo informático	Artigo 154-A do Código Penal
Enviar uma mensagem para terceiros com informação considerada confidencial	Divulgação de segredo	Artigo 153 do Código Penal
Enviar um vírus que comprometa equipamento ou conteúdo de terceiros	Dano	Artigo 163 do Código Penal
Copiar um conteúdo e não mencionar a fonte, ou baixar arquivos de mídia (MP3, AVI, entre outros) que não possua controle de direitos autorais	Violação de direito autoral	Artigo 184 do Código Penal
Enviar mensagem de correio eletrônico com remetente falso	Falsa identidade	Artigo 307 do Código Penal
Fazer cadastro com nome ou informações falsas em sítios de internet ou sistemas computacionais	Inserção de dados falsos em sistemas de informação	Artigo 313-A do Código Penal
Entrar em sistema de informação e modificar um conteúdo sem autorização	Adulterar dados em sistemas de informação	Artigo 313-B do Código Penal
Participar de jogos de azar via internet (por exemplo, cassino on-line)	Jogo de azar	Artigo 50 da Lei de Contravenções Penais

Exemplo de infração	Tipo de crime	Enquadramento jurídico
Adquirir ou transmitir fotos de crianças e adolescentes nuas	Pedofilia (pornografia infantil)	Artigos 241-A e 241-B do Estatuto da Criança e do Adolescente
Usar logomarca de empresa em mensagem de correio eletrônico, documentos, propostas ou contratos sem autorização do titular, no todo ou em parte, ou imitá-la de modo que possa induzir a confusão	Crime contra a propriedade industrial	Artigo 195 do Código de Propriedade Industrial
Uso de mecanismos (softwares ou ferramentas diversas) para coleta de informações sem autorização prévia	Interceptação telemática	Artigo 10 da Lei 9296/96
Usar cópia de software sem licença ("pirata")	Pirataria	Artigo 12 da Lei 9609/98

Fonte: Adaptado de Ferreira (2008).

5.3 Papel dos profissionais da segurança da informação

Dentro das organizações existem grandes desafios aos gestores que desejam implementar uma boa política de segurança da informação. Um destes desafios é encontrar profissionais capacitados com especializações na área. A alta administração deve ter um conhecimento mínimo sobre o papel destes profissionais especialistas em segurança da informação.

Primeiramente estes profissionais estarão envolvidos com diversos setores da organização, recebendo e emitindo opiniões sobre todas as atividades desenvolvidas, processos e as formas de assegurar a segurança da informação em todos estes aspectos. Não precisam necessariamente possuir um vasto conhecimento *hacker* para garantir o bom desempenho de suas atividades, até porque aquele que sabe invadir não necessariamente saberá defender.

Visto que incidentes de segurança podem afetar um negócio de forma séria, e até mesmo irreparável, o papel destes profissionais é uma poderosa ferramenta para diminuir pontos vulneráveis que geram estes incidentes. As habilidades destes profissionais incluem desde a execução, coordenação, gerenciamento de projetos até planejamento estratégico e apresentação executiva de resultados junto à alta administração. Outras responsabilidades destes profissionais incluem:

- × definição da abordagem estratégica que será adotada para a organização;
- × definição da forma de atuação do grupo de segurança;
- × ter por base as normas e melhores práticas do mercado;
- × proteção dos ativos de informação;
- × definição de controles para novas iniciativas;
- × acompanhamento da eficácia da política de segurança na organização;

Um destes profissionais tem um destaque especial, por efetuar o papel de coordenação da equipe de segurança, o denominado *Security Officer*, ou agente de segurança. Seu papel não será de substituir os técnicos especialistas, até porque possuir uma equipe heterogênea na área de segurança pode ser um bom diferencial para a organização. O *Security Officer* personifica o papel de gestor e, segundo Ferreira (2008) deve possuir também as seguintes qualificações:

- a) **excelente capacidade de comunicação** – como o gestor de segurança da informação necessita manter os executivos da alta administração devidamente informados, deve ter uma boa capacidade de comunicação escrita e também de oratória. Tais habilidades são necessárias em momentos nos quais será necessário convencer os gestores da necessidade de investimento em recursos de proteção lógica, física, bem como ferramentas de segurança. Não poderá, por exemplo, usar termos técnicos incompreensíveis para leigos, devendo fazer a devida tradução de forma que seja facilmente com-

preensível por parte de pessoas que não possuem o mesmo conhecimento técnico que ele.

- b) **capacidade de conciliar os interesses de segurança com os interesses do negócio** – tal profissional deverá ter a capacidade de escolher, dentre as diversas ferramentas e soluções de segurança disponíveis no mercado, a que melhor se enquadra nos objetivos de negócio da organização. Nem sempre o produto mais caro será o melhor, pois o mesmo deve adequar-se primariamente às necessidades que o negócio impõe.
- c) **capacidade de ser autodidata** – profissionais desta área devem possuir um grande interesse pelo aperfeiçoamento pessoal, sendo proativo em relação às tecnologias e produtos disponíveis atualmente. Devido às rápidas mudanças de tecnologias e soluções de segurança, este profissional deve possuir uma grande rede de contatos de especialistas no tema, mantendo-se constantemente atualizado.
- d) **familiaridade com termos e conceitos da área** – termos como alta disponibilidade, SLA, Acordo de Confidencialidade, bem como conceitos de *firewall*, *PKI*, *IDS* e *Single-Sign-On* (SSO) fazem parte da rotina e do conhecimento mínimo que este profissional deve possuir, principalmente como responsável pela implementação de um Sistema de Gestão de Segurança da Informação (detalhado no capítulo 2).
- e) **certificações e especializações na área** – bons profissionais, independente da área que atuam, têm algumas características peculiares: buscam capacitação constante e estão sempre atualizados frente às últimas novidades de sua área de atuação. Para a segurança da informação, as certificações, cursos e especializações são parte fundamental da formação do profissional. Destacamos no quadro a seguir as principais certificações requisitadas na área de segurança da informação em 2015:

Quadro 5.2 - Certificações mais requisitadas na área de segurança da informação

Certificação	Descrição
Information Systems Security Engineering Professional (ISSEP/CISSP)	Desenvolvida em conjunto com a Agência de Segurança dos EUA (NSA), a Information Systems Security Engineering Professional (ISSEP) abrange a integração de metodologias e melhores práticas de segurança em todos os sistemas de informação, incluindo projetos, aplicações e práticas de negócios.
EC-Council Licensed Penetration Tester	A certificação LPT demonstra a capacidade de um profissional de auditoria em segurança de rede para realizar testes de invasão e recomendar ações corretivas para quaisquer deficiências encontradas.
GIAC Certified Penetration Tester	A certificação GPEN é para profissionais de segurança que avaliam redes e sistemas alvo para encontrar vulnerabilidades.
GIAC Security Essentials	A certificação GSEC é para profissionais que querem demonstrar que estão qualificados para aplicações de tarefas de segurança relacionadas a uma ampla gama de sistemas de TI.
Cybersecurity Forensic Analyst	O CSPA prova que os detentores de seu certificado podem conduzir uma análise global dos sistemas de informação, interpretar apropriadamente a evidência e entregar resultados das investigações para os acionistas da empresa de forma eficaz e eficiente. A certificação também demonstra que os profissionais possam realizar essas análises dentro de um prazo limitado.
EC-Council Certified Secure Programmer	A maioria das vulnerabilidades de software são devido a erros de programação. A ECSP tem provado que eles podem desenvolver código de alta qualidade que faz uso das melhores práticas de programação para proteger contra vulnerabilidades.
Check Point Certified Security Expert	A CCSE ensina profissionais de segurança como construir, modificar, implementar e solucionar problemas de verificação de segurança em sistemas no sistema operacional Gaia.

Certificação	Descrição
Certified Secure Software Lifecycle Professional	O CSSLP valida a capacidade do profissional para desenvolver protocolos de aplicação e segurança de software dentro de suas organizações e reduzir vulnerabilidades.

Fonte: <https://seginfo.com.br/>.

Síntese

Embora seja imprescindível que o administrador de TI implemente tecnologias fundamentais para a garantia da segurança da informação, não se pode esquecer do elo mais fraco: o fator humano. Estudamos neste capítulo as técnicas de engenharia social mais comumente utilizadas para ataques, e como se proteger destas. Também compreendemos quais procedimentos devem ser adotados pela organização em casos de violações de segurança.

Por fim, orientamos a respeito do perfil do profissional especialista na área de segurança da informação e como este pode auxiliar as organizações na proteção de seus dados.

Atividades

1. Explique resumidamente quais são as etapas do ciclo de vida da Engenharia Social.
2. No contexto da segurança da informação, o termo “engenharia social” se refere a (questão de Concurso Público, TJSC 2009, Analista Jurídico):
 - a) Conjunto de práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas, através da persuasão e se aproveitando da ingenuidade ou confiança das pessoas.
 - b) Conjunto de recomendações que permitem a um administrador do computador acessar informações sobre novas versões do Windows, através da utilização das teclas de atalho “CTRL-S”.

- c) Série de normas que ensinam, dentre outras coisas, a identificar as pessoas responsáveis pela criação de vírus e outras ameaças eletrônicas.
 - d) Estratégia de proteção contra vírus, que consiste em distribuir versões gratuitas de programas antivírus, por e-mail, para todos os endereços da lista de contatos do usuário.
 - e) Prática recomendada pela “Organização Mundial de Segurança”, segundo a qual o procedimento de atualização dos programas anti-vírus deve ser realizado por usuários diferentes a cada vez.
3. O que é *phishing* e como se proteger deste ataque?
4. Qual é a área de atuação do profissional LPT (*Licensed Penetration Tester*)?

6

Gerenciamento de Riscos em Segurança da Informação

JÁ ESTUDAMOS NOS capítulos anteriores o papel estratégico que as informações possuem em uma organização. Neste capítulo aprenderemos a mensurar os riscos associados à segurança da informação em sistemas, de forma que os administradores possam tomar decisões baseados em análises que seguem metodologias conhecidas no mercado corporativo.

APRENDEREMOS A IMPORTÂNCIA do gerenciamento de riscos, bem como sua integração com o ciclo de vida de desenvolvimento de um sistema. Também detalharemos uma metodologia de avaliação de riscos, por meio de etapas bem definidas. Finalmente, abordaremos estratégias e opções para mitigação dos riscos inerentes à segurança dos sistemas informatizados em uma organização.

Objetivo de aprendizagem:

- × Ser habilitado a identificar, tratar e monitorar continuamente os riscos associados à segurança da informação.

6.1 Introdução ao gerenciamento de riscos em segurança da informação

Existem diversas formas de classificação para a gestão de riscos associados à segurança da informação. Esta gestão caracteriza-se como base importante para a elaboração e conteúdo de uma política de segurança da informação em uma organização, visto que as mesmas já têm percebido que a existência de riscos, sem o devido tratamento, são prejudiciais aos resultados, pois sua ocorrência pode afetar as operações do negócio.

Para fins didáticos, utilizaremos como base o Guia SP-800-30 – *Risk Management Guide for Information Technology Systems* do NIST. O National Institute of Standards and Technology (NIST) faz parte do Departamento de Comércio dos Estados Unidos da América. Tem como principal objetivo a promoção de padrões equitativos, ampliando a competitividade industrial a fim de promover a qualidade de vida.

6.2 Importância do gerenciamento de riscos

O gerenciamento de riscos no contexto de TI é o processo que habilita os administradores a identificar, priorizar e avaliar os custos operacionais de implantação de medidas de proteção aos sistemas de informação, bem como os dados que dão suporte à missão de uma organização.

Tal processo não se limita somente ao contexto de TI, mas em vários outros aspectos de uma organização ou pessoa. Por exemplo, no caso de uma pessoa que decide investir em um sistema de segurança doméstico, pagando um valor contratual mensal a uma determinada empresa prestadora de serviços nesta área. Presume-se que o proprietário desta residência avaliou o custo-benefício desta medida, pois levou em consideração o risco de não fazê-la. Portanto, o proprietário desta residência efetuou uma avaliação de risco e

tomou uma decisão de proteger o seu patrimônio investindo um determinado valor para tal fim.

No contexto corporativo, cada organização possui uma missão fundamental, e os gestores, sejam eles chefes diretos ou diretores, devem assegurar o cumprimento desta missão por parte de todos os seus subordinados. São os proprietários e guardadores da missão fundamental de uma organização que devem determinar as capacidades de segurança que seus sistemas de TI devem possuir para fornecer o nível desejado de suporte à missão, diante das ameaças de segurança atuais. A grande maioria das organizações não possui um alto orçamento disponível para o investimento em segurança de TI, portanto os gastos em segurança devem passar por revisão detalhada, assim como outras decisões gerenciais. Quando uma metodologia de gestão de riscos bem estruturada é aplicada com eficiência, isto auxilia a alta administração a fornecer suporte de segurança essencial ao cumprimento da missão organizacional.

6.2.1 Integração com ciclo de vida de desenvolvimento de sistemas

Uma das principais razões que motivam uma organização a implementar um processo de gerenciamento de riscos para seus sistemas de TI é a necessidade de minimizar os impactos negativos em caso de incidentes que comprometam a continuidade dos negócios desta. Outro fato relevante é que a tomada de decisões neste tipo de situação exige uma base sólida e bem definida. Para que isto seja efetivo, também é necessário que o gerenciamento de riscos esteja integrado de forma plena ao Ciclo de Vida de Desenvolvimento de Sistemas (SDLC – *Systems Development Life Cycle*). Embora exista variabilidade nos modelos de CVDS, trabalharemos com um modelo de cinco fases, para fins de integração com gerenciamento de riscos: iniciação, desenvolvimento ou aquisição, implementação, operação ou manutenção e eliminação.

Existem casos em que um sistema de informação pode estar presente em mais de uma fase ao mesmo tempo. Independentemente disto, a metodologia de gerenciamento de riscos permanece inalterada, não importando a fase do CVDS à qual está submetida. O gerenciamento de riscos é um processo que pode ser realizado de forma iterativa para cada fase principal do CVDS.

O quadro 6.1 descreve as características das fases e indica como o gerenciamento de risco pode ser realizado em integração com cada fase:

Quadro 6.1 – Fases do CVDS e integração com gerenciamento de riscos

Fase	Descrição	Integração com gerenciamento de riscos
1 – Iniciação	A necessidade de um sistema de informação é expressa, e a finalidade e escopo do mesmo são documentados	Os riscos identificados são usados para suportar o desenvolvimento dos requisitos do sistema, incluindo os requisitos de segurança, e conceitos de segurança de operações
2 – Desenvolvimento ou aquisição	O sistema de informação é desenvolvido ou adquirido	Os riscos identificados durante esta fase podem ser usados para apoiar as análises de segurança do sistema
3 – Implementação	Os recursos de segurança do sistema devem ser configurados, habilitados, testados e verificados	O processo de gerenciamento de riscos apoia a avaliação da implementação do sistema em relação às suas necessidades e dentro do seu ambiente operacional modelado. As decisões relativas aos riscos identificados devem ser feitas antes da operação do sistema
4 – Operação ou manutenção	O sistema executa suas funções. Normalmente, o sistema está sendo modificado de forma contínua por meio da adição de hardware e software e por mudanças nos processos organizacionais, políticas e procedimentos	As atividades de gerenciamento de risco são realizadas periodicamente para revalidação ou sempre que grandes mudanças são feitas a um sistema de informação em seu ambiente operacional de produção (por exemplo, novas interfaces de sistema)

Fase	Descrição	Integração com gerenciamento de riscos
5 – Eliminação	Esta fase pode envolver o descarte de informações, hardware e software. As atividades podem incluir mover, arquivar, descartar ou destruir informações e sanitizar o hardware e o software (efetuar o descarte seguro)	As atividades de gerenciamento de risco são executadas para componentes do sistema que serão descartados ou substituídos para garantir que o hardware e software serão eliminados corretamente, que os dados residuais serão devidamente tratados e que a migração do sistema é conduzida de forma segura e sistemática

Fonte: NIST SP-800-30 (2002).

6.3 Avaliação de riscos

O processo de avaliação de riscos é o primeiro passo da metodologia de gerenciamento de riscos. A avaliação de risco tem por objetivo apontar às organizações qual é a extensão de uma potencial ameaça e o risco associado, a um sistema de informações dentro do seu ciclo de vida de desenvolvimento. Este processo trará um resultado que irá ajudar na identificação dos controles apropriados para redução ou eliminação dos riscos durante a próxima etapa: o processo de mitigação de riscos (detalhado no tópico 6.4).

O risco é a mensuração da probabilidade de uma determinada ameaça explorar uma vulnerabilidade potencial, bem como o impacto resultante deste evento em uma organização. A determinação da probabilidade de ocorrência de um evento adverso futuro se dá quando são analisadas as ameaças a um sistema de informação juntamente com as vulnerabilidades potenciais e os controles em vigor para o sistema em questão. O impacto é a mensuração da magnitude de um dano causado por uma vulnerabilidade explorada. O nível de impacto tem profunda relação com os potenciais impactos à missão da organização, produzindo assim um valor relativo para os ativos e recursos de TI afetados. Isto inclui a criticidade e a sensibilidade dos componentes e dados do sistema de TI. A metodologia de avaliação de riscos engloba nove

etapas primárias, elencadas a seguir, e que serão detalhadas nos itens 6.3.1 a 6.3.9 (NIST SP-800-30, 2002).

- × Etapa 1 – caracterização dos sistemas;
- × Etapa 2 – identificação das ameaças;
- × Etapa 3 – identificação das vulnerabilidades;
- × Etapa 4 – análise dos controles de segurança;
- × Etapa 5 – determinação da probabilidade;
- × Etapa 6 – análise de impacto;
- × Etapa 7 – determinação do risco;
- × Etapa 8 – recomendações dos controles de segurança;
- × Etapa 9 – documentação dos resultados.

6.3.1 Etapa 1 – caracterização dos sistemas

Para condução da avaliação dos riscos para um sistema de informação, o primeiro passo é definir o escopo e a abrangência. Nesta etapa, os limites do sistema são identificados, juntamente com os recursos e as informações que constituem o mesmo. Caracterizar um sistema de informação estabelece o escopo do esforço de avaliação de riscos, delimita os limites operacionais de autorização e fornece informações essenciais para a definição do risco, como por exemplo: hardware, software, conectividade do sistema e responsáveis pelo suporte.

A seguir descrevemos as informações relacionadas e utilizadas para caracterizar um sistema de informação e seu ambiente operacional, sugerindo técnicas de coleta de informações que podem ser usadas para solicitar informações relevantes para o ambiente de processamento.

A metodologia estudada neste tópico pode ser aplicada a avaliações de sistemas únicos ou múltiplos, e também inter-relacionados. Neste último caso, é importante que o domínio de interesse e todas as interfaces e dependências sejam definidos antes da aplicação da metodologia.

× **Informações relacionadas aos sistemas**

Identificar os riscos em um sistema de informação requer uma compreensão profunda de seu ambiente de processamento e fina-

lidade. Os profissionais que conduzem a avaliação de risco devem, portanto, primeiro coletar informações relacionadas ao sistema, que geralmente são classificadas da seguinte forma:

- ✗ hardware;
- ✗ software;
- ✗ interfaces (internas ou externas);
- ✗ dados e informações;
- ✗ pessoas que fornecem suporte e utilizam o sistema;
- ✗ missões do sistema;
- ✗ criticidade dos dados e sistemas (nível de proteção necessário).

Informações adicionais relacionadas ao ambiente operacional do sistema de informação incluem, mas não se limitam a:

- ✗ necessidades funcionais do sistema;
- ✗ usuários do sistema;
- ✗ políticas de segurança;
- ✗ arquitetura de segurança;
- ✗ topologia de rede;
- ✗ recursos atuais utilizados para proteger as informações contra perda de confidencialidade, integridade e disponibilidade;
- ✗ fluxo das informações como: interfaces, entrada e saída de dados;
- ✗ controles de segurança como: produtos para identificação e autenticação, controle de acesso, auditoria, criptografia;
- ✗ controles gerenciais como: regras de comportamento, planejamento de segurança;
- ✗ controles operacionais como: segurança de pessoal, backup, planos de continuidade, contingências, manutenção dos sistemas, inclusão/exclusão de usuários e segregação de funções;
- ✗ segurança física e do ambiente.

Quando um sistema encontra-se na fase de desenvolvimento, é possível obter as informações relacionadas a partir da documentação de análise de requisitos. Informações relevantes sobre a segurança do sistema podem ser obtidas nos documentos de projeto e plano de segurança.

Se o sistema já está em operação, estas informações a respeito da segurança do mesmo podem ser obtidas em procedimentos documentados e não documentados, bem como em dados sobre configuração de ambiente e conectividade de rede (NIST SP-800-30, 2002).

× **Técnicas para obtenção de informações**

Existem algumas técnicas que podem ser usadas na coleta de informações relevantes para o sistema de informação, dentre elas podemos citar:

- × **questionários** – responsáveis pela avaliação de risco podem elaborar um questionário sobre os controles de gestão e de funcionamento planejados ou utilizados para o sistema em questão;
- × **entrevistas no local** – entrevistas com os responsáveis pelo suporte e gerenciamento podem revelar informações úteis, por exemplo, como o sistema é operado e gerenciado;
- × **revisão de documentação** – documentos como manuais, projeto, requisitos, entre outros, podem fornecer informações relevantes sobre os controles de segurança utilizados;
- × **ferramentas automatizadas de escaneamento** – existem ferramentas e métodos proativos que podem auxiliar no mapeamento do sistema de forma eficiente.

Vale ressaltar que este processo de coleta de informações pode ser conduzido durante todas as etapas de avaliação e análise de risco.

Importante

O produto final da etapa 1 é a definição dos sistemas analisados sobre suas limitações, funcionalidades, criticidade e sensibilidade.

6.3.2 Etapa 2 – identificação das ameaças

As ameaças são possibilidades de um agente mal-intencionado ou evento inesperado explorar uma vulnerabilidade de forma eficaz. A vulnerabilidade é uma fraqueza que pode ser accidentalmente utilizada ou intencionalmente explorada. Quando não existe vulnerabilidade que pode ser explorada a ameaça não representa risco.

Nas seções seguintes vamos considerar fontes de ameaças em potencial, vulnerabilidades e controles existentes a fim de determinar a probabilidade de uma ameaça.

- » **Identificação da fonte de ameaças**

Este passo consiste em identificar efetivamente a fonte das ameaças, destacando as ameaças que são aplicáveis ao ambiente avaliado. Elas podem ser definidas como qualquer evento ou circunstância que possa causar danos ao sistema de informação. As mais comuns são falhas humanas, causas naturais ou ambientais.

A motivação e os recursos que podem levar à execução de um ataque fazem dos funcionários a maior fonte de ameaças. A revisão do histórico dos incidentes de segurança pode ajudar a identificar as fontes humanas de ameaças que podem causar danos potenciais ao ambiente. O quadro 6.2 a seguir apresenta um resumo das ameaças mais comuns, principais motivações e os métodos ou ações utilizadas.

Quadro 6.2 – Ameaças, motivações e ações utilizadas

Fontes de ameaça	Motivação	Ações utilizadas
Hacker, cracker	Desafio, ego, rebeldia	<i>Hacking</i> , engenharia social, invasão de sistema, acesso não autorizado a sistemas
Criminoso de computador	Destrução de informação, divulgação e alteração não autorizada de informações, retorno financeiro	Crime por computador (espionagem), atos fraudulentos (interceptação de informações), suborno, invasão de sistemas

Fontes de ameaça	Motivação	Ações utilizadas
Terrorista	Chantage, destruição, vingança, exploração	Bombas, terrorismo, guerra de informação, ataques de negação de serviços
Espionagem industrial	Vantagem competitiva, espionagem	Exploração econômica, roubo de informações, engenharia social, invasão de sistemas, acesso a informações classificadas
Funcionários da própria organização (aqueles que não recebem treinamento adequado, negligentes, desonestos e demitidos)	Curiosidade, ego, inteligência, retorno financeiro, vingança, erros não intencionais	Abuso dos recursos de TI, roubo e fraude, inclusão de dados falsos, interceptação, inclusão de códigos maliciosos, venda de informações, falhas nos sistemas, acesso não autorizado aos sistemas

Fonte: NIST SP-800-30 (2002).

Importante

O produto final da etapa 2 é uma lista de fontes de ameaças que podem explorar as vulnerabilidades de um determinado sistema, a denominada "declaração de ameaças".

6.3.3 Etapa 3 – identificação das vulnerabilidades

Nesta etapa são identificadas as vulnerabilidades do sistema que podem ser exploradas pelas potenciais fontes de ameaças. Um exemplo de vulnerabilidade que pode ser listado é o fato dos usuários demitidos não serem bloqueados nos sistemas de informação.

As vulnerabilidades, técnicas ou não, associadas com o ambiente de TI podem ser identificadas por meio de técnicas para obtenção de informações. A internet apresenta-se também como uma rica fonte de informações, visto que no site de fabricantes de ferramentas e softwares utilizados no ambiente

de TI encontram-se *patches* e *hot fixes* (atualizações de segurança) que diminuem ou eliminam as vulnerabilidades.

✗ **Testes de segurança do sistema**

Os métodos proativos, que empregam testes de segurança do sistema, podem ser usados para identificar eficientemente as vulnerabilidades, criticidade e os recursos disponíveis do sistema. Os métodos de teste podem incluir:

- ✗ ferramenta automatizada de verificação de vulnerabilidades;
- ✗ teste de segurança e avaliação;
- ✗ teste de penetração (*pentest*).

As ferramentas de varredura de vulnerabilidades verificam um grupo de *hosts* em uma rede de maneira automatizada, identificando as potenciais vulnerabilidades conhecidas. É preciso tomar cuidado com os falsos positivos, ou seja, alertas de vulnerabilidades identificadas pela ferramenta que não representam ameaça real no ambiente do sistema.

Os testes de segurança e avaliação devem incluir o desenvolvimento e a execução de um plano de teste. Neste plano incluem-se *scripts* de teste, procedimentos e resultados esperados. Os testes de segurança do sistema têm como objetivo testar a eficácia dos controles de segurança, assim como a garantia de que os controles que estão sendo aplicados atendem às especificações de segurança.

Existem testes de segurança opcionais que podem ser aplicados na identificação de vulnerabilidades de um sistema. Um destes teste é o *pentest* (teste de penetração). Caracteriza-se por ser um teste de invasão ativo, em que um atacante tentará burlar as barreiras de segurança, avaliando a capacidade do sistema de resistir a ataques que visam contornar a segurança deste.

Importante

O produto final da etapa 3 é a relação das vulnerabilidades encontradas no sistema que podem ser exploradas por potenciais fontes de ameaça.

6.3.4 Etapa 4 – análise dos controles de segurança

O objetivo desta etapa é analisar os controles que foram implementados ou planejados para serem implementados pela organização para minimizar ou eliminar a probabilidade de uma ameaça explorar uma vulnerabilidade do sistema.

Para obter uma classificação geral que indique a probabilidade de que uma potencial vulnerabilidade possa ser explorada, a implementação de controles atuais ou planejados deve ser considerada. Por exemplo, não é provável que uma vulnerabilidade seja explorada se houver um baixo nível de interesse ou capacidade de fonte de ameaça ou se houver controles de segurança efetivos que possam eliminar ou reduzir a magnitude do dano.

- × **Métodos de controle**

Os controles de segurança englobam a utilização de métodos técnicos e não-técnicos. Os controles técnicos são aqueles que são incorporados no hardware, software ou *firmware* (por exemplo, mecanismos de controle de acesso, identificação e autenticação, criptografia, software de detecção de intrusão). Os controles não-técnicos são controles gerenciais e operacionais, tais como políticas de segurança, procedimentos operacionais, segurança pessoal, física e ambiental.

- × **Categorias de controle**

As categorias de controle podem ser classificadas como:

- × **controles preventivos** – inibem tentativas de violação às políticas de segurança e incluem mecanismos avançados de controle de acesso, criptografia e autenticação;
- × **controles detectivos** – alertam as tentativas ou efetivas violações de políticas de segurança e incluem trilhas de auditoria e mecanismos de detecção de intrusos;
- × **Técnicas para analisar os controles de segurança**

O desenvolvimento de *checklists* (listas de verificação) de requisitos de segurança pode ser útil na análise de controles. Todavia é essencial atualizar estes *checklists* para refletir as mudanças no ambiente

do sistema de uma organização (por exemplo, alterações nas políticas de segurança, métodos e requisitos) para garantia da eficácia dos trabalhos.

Importante

O produto final da etapa 4 é a relação dos controles de segurança utilizados e planejados para minimizar a probabilidade de uma vulnerabilidade ser explorada visando reduzir o impacto caso ela ocorra.

6.3.5 Etapa 5 – determinação da probabilidade

Alguns fatores devem ser considerados para a determinação da classificação que indique a probabilidade de exploração de uma vulnerabilidade em potencial. Tais fatores são: motivação e capacidade da fonte de ameaça; natureza da vulnerabilidade; existência e eficácia dos controles de segurança atuais.

A probabilidade de que uma potencial vulnerabilidade possa ser explorada por uma determinada fonte de ameaça pode ser descrita como alta, média ou baixa. O quadro a seguir descreve estes três níveis:

Quadro 6.3 – Níveis de probabilidade

Nível	Definição
Alto	A fonte de ameaça está altamente motivada e possui conhecimento suficiente para execução do ataque. Os controles de segurança para prevenir que a vulnerabilidade seja explorada são ineficazes.
Médio	A fonte de ameaça está motivada e possui conhecimento suficiente para execução do ataque. Os controles de segurança para prevenir que a vulnerabilidade seja explorada são eficazes
Baixo	A fonte de não ameaça está altamente motivada e não possui conhecimento suficiente para execução do ataque. Os controles de segurança para prevenir que a vulnerabilidade seja explorada são eficazes.

Fonte: NIST SP-800-30 (2002).



Importante

O produto final da etapa 5 é a definição do nível de probabilidade: alto, médio ou baixo.



6.3.6 Etapa 6 – análise de impacto

O próximo passo é determinar o impacto resultante no caso de uma ameaça obter sucesso em explorar uma vulnerabilidade. Antes de iniciar a análise de impacto, é necessário ter em mãos as informações que foram levantadas na etapa de Caracterização dos Sistemas.

Se estas documentações não existirem, a criticidade do sistema e dos dados pode ser determinada com base no nível de proteção necessário para manter a confidencialidade, integridade e disponibilidade. Independentemente do método usado para determinar o grau de criticidade de um sistema de informação e seus dados, os proprietários são os principais responsáveis pela determinação do nível de impacto para seu próprio sistema e informações. Consequentemente, na análise do impacto, a abordagem apropriada é entrevistar o administrador do sistema e os proprietários da informação. Podemos concluir que o impacto resultante de um evento de segurança pode ser descrito em termos de perda ou degradação da combinação de qualquer um dos seguintes três objetivos de segurança: confidencialidade, integridade e disponibilidade.

Existem alguns impactos que podem ser quantificados de forma mais visível quando há perda de receita, bem como nos valores que deverão ser despendidos para reparação do sistema, além do custo em esforço humano necessário para correção dos problemas causados por incidentes de segurança. Também existem perdas causadas por incidentes de segurança, que dificilmente poderão ser mensurados em termos monetários. Entre elas podemos citar a perda de confiança do público, bem como a perda de credibilidade da organização. Os impactos que não podem ser mensurados em unidades específicas são descritos em termos de impactos altos, médios e baixos. O quadro a seguir detalha estes níveis de impacto.

Quadro 6.4 – Níveis de impacto

Nível	Definição
Alto	Perda significante dos principais ativos e recursos; perda da reputação, imagem e credibilidade; impossibilidade de continuar com as atividades do negócio
Médio	Perda dos principais ativos e recursos; Perda da reputação, imagem e credibilidade
Baixo	Perda de alguns dos principais ativos e recursos; pequena perda da reputação, imagem e credibilidade

Fonte: adaptado de NIST SP-800-30 (2002).

Importante

O produto final da etapa 6 é a definição do nível de impacto: alto, médio ou baixo.

6.3.7 Etapa 7 – Determinação do risco

Esta etapa tem como objetivo a avaliação do nível de risco dos sistemas. A determinação do risco de uma ameaça específica pode ser expressada da seguinte forma (NIST SP-800-30, 2002):

- × a probabilidade de ocorrência;
- × o nível de impacto causado pelo sucesso da exploração de uma vulnerabilidade;
- × a eficácia dos controles de segurança existentes para minimizar os riscos;

Para a determinação do risco de forma mais precisa, é necessária a criação de uma matriz de riscos, exemplificada a seguir:

- × **Matriz de nível de risco**

Obtemos a determinação do risco (entre alto, médio ou baixo) multiplicando a classificação da probabilidade da ocorrência *versus* o impacto na organização. A tabela 6.1 demonstra a forma de cálculo:

Tabela 6.1 – Matriz do nível de risco

PROBABILIDADE	IMPACTO		
	Baixo (10)	Médio (50)	Alto (100)
Alto (1,0)	10	50	100
Médio (0,5)	5	25	50
Baixo (0,1)	1	5	10

Fonte: NIST SP-800-30 (2002).

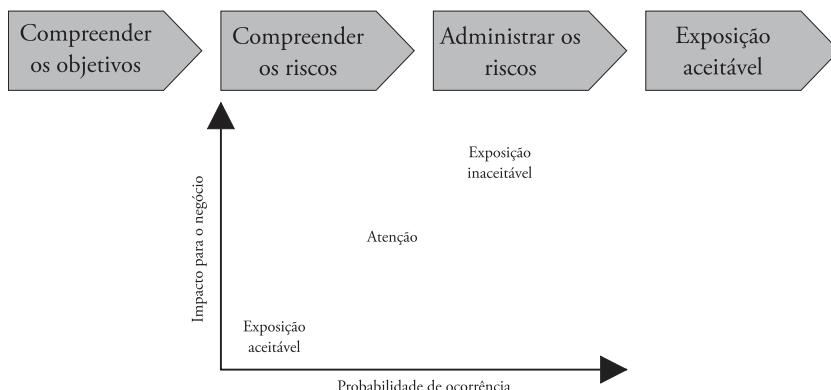
A escala de risco fica da seguinte forma:

- × alto – pontuação entre 51 e 100;
- × médio – pontuação entre 11 e 50;
- × baixo – pontuação entre 1 e 10.

Para diminuir a exposição aos riscos mais relevantes, pode-se adotar a estratégia da identificação do impacto que os riscos podem oferecer às atividades da organização, assim como sua probabilidade de ocorrência, mediante a seguinte análise:

Figura 6.1 – Análise matriz de nível de risco

Riscos (objetivos) – Controles = Exposição



Fonte: Adaptado de Ferreira (2008).

O quadro a seguir descreve os níveis de risco calculados na matriz anterior. Se uma determinada vulnerabilidade for explorada o sistema estará exposto a um determinado nível de risco, podendo ser este nível alto, médio ou baixo. A escala de risco também apresenta ações que a alta administração deve tomar para cada nível de risco apresentado.

Quadro 6.5 – Níveis de risco e ações

Nível	Definição
Alto	Se uma observação ou descoberta é avaliada como de alto risco, há uma forte necessidade de medidas corretivas. Um sistema existente pode continuar a funcionar, mas um plano de ação corretivo deve ser posto em prática o mais rápido possível.
Médio	Se uma observação ou descoberta é classificada como de risco médio, são necessárias ações corretivas e um plano deve ser desenvolvido para incorporar essas ações dentro de um período de tempo razoável.
Baixo	Se uma observação ou descoberta é descrita como de baixo risco, o administrador do sistema deve determinar se as ações corretivas ainda são necessárias ou decidir aceitar o risco.

Fonte: NIST SP-800-30 (2002).

Importante

O produto final da etapa 7 é a definição do nível de risco: alto, médio ou baixo.

6.3.8 Etapa 8 – recomendações dos controles de segurança

Durante esta etapa, são fornecidos controles que podem mitigar ou eliminar os riscos identificados. O objetivo dos controles recomendados é reduzir o nível de risco para o sistema de informação e seus dados a um nível aceitável.

Os seguintes fatores devem ser considerados na recomendação de controles e soluções alternativas para minimizar ou eliminar os riscos identificados:

- × eficácia das opções recomendadas (por exemplo, compatibilidade com o sistema);
- × legislação e regulamentação;
- × política organizacional;
- × impacto operacional;
- × segurança e confiabilidade.

As recomendações de controle são o resultado do processo de avaliação de risco e contribuem para o processo de mitigação de riscos, durante o qual os controles de segurança técnica e procedimentos recomendados são avaliados, priorizados e implementados.

Deve-se notar que nem todos os possíveis controles recomendados podem ser implementados para reduzir a perda. Para determinar quais são necessários e apropriados para uma organização específica, uma análise de custo-benefício deve ser conduzida para os controles propostos, a fim de demonstrar que os custos de implementação dos controles podem ser justificados pela redução do nível de risco. Além disso, o impacto operacional (por exemplo, o efeito sobre o desempenho do sistema) e a viabilidade (por exemplo, requisitos técnicos, aceitação do usuário) de introduzir a opção recomendada devem ser cuidadosamente avaliados durante o processo de mitigação de riscos.

Importante

O produto final da etapa 8 são recomendações de controles e soluções alternativas para mitigar os riscos.

6.3.9 Etapa 9 – documentação dos resultados

Uma vez concluída a avaliação dos riscos (identificadas as ameaças e as vulnerabilidades, e os controles recomendados fornecidos), os resultados devem ser documentados em um relatório oficial. Um relatório de avaliação

de risco é um relatório de gestão que ajuda a alta administração a tomar decisões sobre políticas, procedimentos, orçamento e mudanças operacionais e de gestão do sistema.

Ao contrário de um relatório de auditoria ou investigação, que procura por irregularidades, um relatório de avaliação de risco não deve ser apresentado de forma acusatória, mas como uma abordagem sistemática e analítica para avaliar o risco de forma que a alta administração compreenda os riscos e possa alocar recursos para reduzir e corrigir potenciais perdas. Por esta razão, alguns especialistas preferem abordar os pares de ameaça/vulnerabilidade como observações em vez de achados no relatório de avaliação de risco.

Importante

O produto final da etapa 9 é o relatório de avaliação de risco, que descreve as ameaças e vulnerabilidades, mede o risco e fornece recomendações para a implementação de controles.

6.4 Mitigação de riscos

A mitigação de riscos envolve priorizar, avaliar e implementar os controles apropriados de redução de risco recomendados no processo de avaliação de risco. Uma vez que a eliminação de todos os riscos é geralmente impraticável ou quase impossível, é responsabilidade dos gestores de negócio usar a abordagem de menor custo e implementar os controles mais apropriados para diminuir o risco a um nível aceitável.

6.4.1 Opções para mitigação de riscos

A mitigação de riscos é uma metodologia usada pela alta administração para reduzir o risco do negócio. Ela pode ser alcançada por meio de uma das seguintes opções a seguir:

- ✗ **aceitação de riscos** – aceitar o risco potencial e continuar operando o sistema de informação ou implementar controles para reduzir o risco para um nível aceitável;

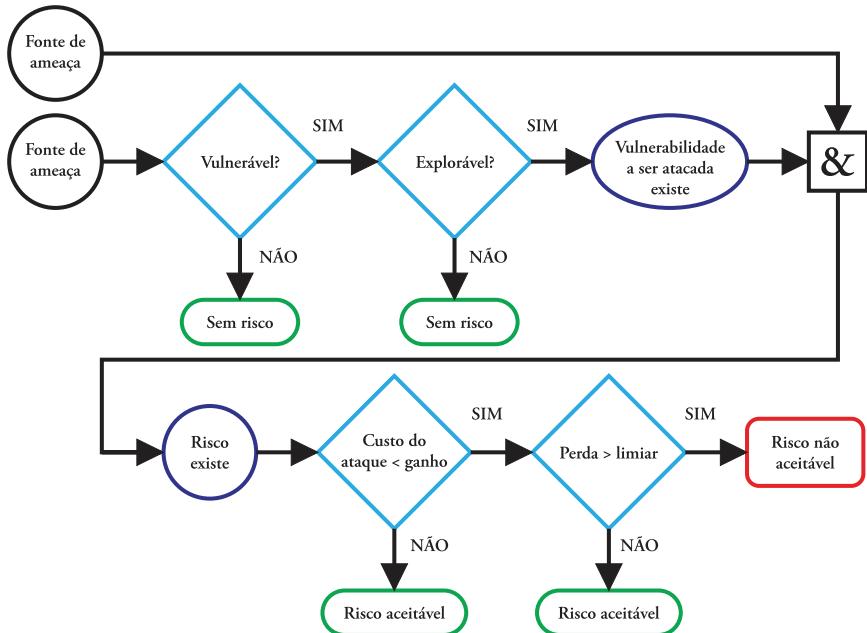
- × **prevenção de riscos** – evitar o risco eliminando a causa e/ou consequência do mesmo (por exemplo, renunciar a determinadas funções do sistema ou desligá-lo quando os riscos são identificados);
- × **limitação de riscos** – limitar o risco por meio da implementação de controles que minimizam o impacto adverso de uma ameaça que está explorando uma vulnerabilidade;
- × **planejamento de riscos** – gerir o risco desenvolvendo um plano de mitigação que priorize, implemente e mantenha controles;
- × **pesquisa e reconhecimento** – reduzir o risco de perda reconhecendo a vulnerabilidade ou falha e pesquisando controles para corrigi-las;
- × **transferência de riscos** – transferir o risco usando outras opções para compensar a perda, como por exemplo, a compra de seguros.

Os objetivos de uma organização devem ser considerados na seleção de qualquer uma dessas opções de mitigação de riscos. Pode não ser prático lidar com todos os riscos identificados, por isso deve ser dada prioridade aos pares de ameaças e vulnerabilidades que têm o potencial de causar impacto ou dano significativo no negócio.

6.4.2 Estratégias de mitigação de riscos

A alta administração, conhecendo os riscos potenciais e os controles recomendados, podem fazer a si mesmos as seguintes perguntas: “quando e em quais circunstâncias devo agir? Quando devo implementar esses controles para mitigar o risco e proteger a nossa organização? A figura a seguir aborda estas questões. Pontos apropriados para implementação de ações de controle são indicados nesta figura pela palavra SIM.

Figura 6.2 – Ações de mitigação de riscos



Fonte: Adaptada de NIST SP-800-30 (2002).

A estratégia apresentada é articulada nas seguintes regras básicas, que fornecem orientação sobre ações para mitigar os riscos de ameaças humanas intencionais.

- ✗ **Quando houver vulnerabilidade:** implementar técnicas de garantia para reduzir a probabilidade de uma vulnerabilidade ser explorada;

- × **Quando uma vulnerabilidade pode ser explorada:** aplicar proteções em camadas, projetos arquitetônicos e controles administrativos para minimizar o risco de evitar essa ocorrência;
- × **Quando o custo do ataque é menor do que o ganho potencial:** aplicar proteções para diminuir a motivação de um atacante, aumentando o custo do ataque (por exemplo, o uso de controles no sistema, como limitar o que um usuário do sistema pode acessar e fazer pode reduzir significativamente o ganho de um atacante);
- × **Quando a perda é muito grande:** aplicar princípios de *design*, desenhos arquitetônicos e proteções técnicas e não-técnicas para limitar a extensão do ataque, reduzindo assim o potencial de perda para a organização.

A estratégia descrita anteriormente, com exceção do terceiro item da lista (pois não há “atacante”, nenhuma motivação ou ganho envolvido) também se aplica à mitigação de riscos decorrentes de ameaças humanas ambientais ou não intencionais, por exemplo, erros do sistema ou do usuário.

6.4.3 Abordagem para implementação de controles

Quando ações de controle necessitam ser implementadas, a seguinte regra se aplica: “abordar os maiores riscos e adotar uma estratégia de mitigação destes ao menor custo possível, com impacto mínimo sobre as outras capacidades da organização” (NIST SP-800-30, 2002).

6.4.4 Análise de custo-benefício

Para alocar recursos e implementar controles, as organizações, após identificar todos os controles possíveis e avaliar sua viabilidade e eficácia, devem realizar uma análise de custo-benefício para cada controle proposto para determinar quais controles são necessários e apropriados para suas circunstâncias.

Esta análise custo-benefício pode ser qualitativa ou quantitativa. A análise qualitativa é subjetiva, pois o propósito é a priorização de riscos medidos na fase de análise, bem como para quais riscos serão necessários efetuar uma

análise quantitativa, ou seja, em termos de valores monetários. O objetivo destas análises é demonstrar que os custos de implementação dos controles podem ser justificados pela redução do nível de risco. Por exemplo, a organização não pode gastar R\$ 1.000,00 em um controle para reduzir um risco de R\$ 200,00 em perdas.

6.5 Avaliação contínua

Na maioria das organizações, a própria rede informatizada continuamente será expandida e atualizada, seus componentes alterados e seus aplicativos substituídos ou atualizados com versões mais recentes. Além disso, mudanças de pessoal ocorrerão e as políticas de segurança provavelmente mudarão ao longo do tempo. Essas mudanças significam que novos riscos irão surgir e riscos previamente mitigados podem voltar a ser uma preocupação. Assim, o processo de gestão de riscos está em constante evolução.

Um programa bem-sucedido de gerenciamento de riscos dependerá principalmente do compromisso da alta administração. Também depende do total apoio e participação da equipe de TI. A equipe de avaliação de riscos deve possuir os conhecimentos necessários para aplicar a metodologia de avaliação de riscos de forma que possam identificá-los corretamente. Não se pode esquecer da conscientização e cooperação dos membros da comunidade de usuários, que devem seguir os procedimentos e cumprir os controles implementados para salvaguardar a missão de sua organização.

Síntese

Neste capítulo aprendemos que as organizações devem mensurar os riscos associados à segurança da informação devido à importância da preservação de sua missão diante das ameaças atuais. Aprendemos uma metodologia de avaliação de riscos em sete etapas, envolvendo desde a identificação das ameaças e vulnerabilidades até a correta análise do impacto e determinação dos riscos. Por fim, uma documentação bem-feita auxiliará os gestores na mitigação destes riscos, preservando assim a organização de sofrer perdas diante de um incidente de segurança.

Atividades

1. Explique a importância da análise de riscos estar presente na primeira fase (iniciação) do Ciclo de Vida de Desenvolvimento de Sistemas.
2. Qual a diferença entre ameaça e vulnerabilidade?
3. Quando um risco existe e o custo do ataque é menor que o ganho, este risco é aceitável?
 - a) Sim
 - b) Não
4. Quais são as cinco fases do Ciclo de Vida de Desenvolvimento de Sistemas, as quais devem ser integradas ao gerenciamento de risco?

7

Fundamentos em Auditoria de Sistemas de Informação

AUDITORIA É UM termo que tem sua etimologia no latim *audire*, e pode ser traduzido como “ouvir” ou “saber ouvir”. A atividade de auditoria data de antes de Cristo, na antiga Suméria, Grécia e nas províncias romanas no primeiro século depois de Cristo, entretanto, a auditoria começou a ser vista como uma prática a ser realizada de maneira sistemática pelos ingleses, quando eles começaram a utilizar o termo *auditing*, do qual deriva o termo em português auditoria. Segundo o dicionário Michaelis (2015), auditoria significa: “repartição ou tribunal onde o auditor desempenha as suas funções; exame analítico, minucioso, relativo às operações contábeis e financeiras de uma empresa ou instituição; procedimento de análise, investigação e validação de um sistema, atividade ou informação”.

A EVOLUÇÃO DA auditoria quase confunde-se com a história da organização das civilizações, da necessidade da cobrança de impostos e do surgimento das grandes corporações. No entanto, a auditoria que surgiu somente com a função de detectar fraudes na área da contabilidade, se expandiu na sua função e área de atuação. Hoje, a auditoria está relacionada a várias áreas, como por exemplo, recursos humanos, segurança e *sistemas de informação*, área que será o foco deste capítulo.

Objetivos da aprendizagem:

- × Compreender conceitos básicos de auditoria de sistemas de informação.

7.1 Histórico

Historicamente não é possível ter um registro preciso do início dos procedimentos de auditoria, algumas formas primitivas, com métodos embrionários, podem ser encontradas no mundo antigo. Claramente a atividade de auditoria não começou sistematizada e com todo o arcabouço existente hoje. Como a maioria das atividades, a auditoria iniciou para suprir uma necessidade específica.

7.1.1 Antiguidade

A auditoria era destinada primariamente a evitar fraudes no pagamento de impostos. É possível encontrar atividades de auditoria em alguns escritos de Aristóteles (BOECKH, 1817), nos quais ele afirma que no Senado de Atenas era escolhido um Conselho composto por dez “*logistae*” e dez “*euthuni*”, designados para verificação das contas dos servidores públicos, com uma especial preocupação na detecção de fraudes.

Na Baixa Idade Média o imperador Carlos Magno (768 - 814), do Sacro Império Romano-Germânico, criou inspetores reais, nominados como *Missi dominici*, que eram como auditores reais (IBRACON, 2007). No século XII, na França, a Coroa designava um funcionário para o qual os barões tinham que fazer a leitura pública de suas contas. Nesta época, o papel do auditor era de alguém designado a verificar se existia uma verdade no que estava sendo declarado. Nesta época ainda não estavam constituídas organizações, escolas ou a sistematização de conhecimento específico para a execução desta atividade, ninguém teria como profissão ser auditor – até porque este termo começou a ser utilizado somente na Inglaterra, após a Revolução Industrial.

Na Idade Média, após o Renascimento, começa a acontecer alguma estruturação, surgindo na Europa várias organizações responsáveis por auditar: o Conselho dos Londrinos, no ano de 1310, em Veneza, o Collegio dei Raxonati,

no ano de 1581, na cidade de Paris, o Tribunal de Contas, no ano de 1640 e na cidade de Milão e Bolonha a Academia dei Ragionieri, no ano de 1658.

Entretanto, a atividade de auditor se estabelece realmente na Inglaterra mercantilista, onde floresciam grandes companhias comerciais e um sistema de imposto baseado no lucro das empresas. Portanto, era necessário que o estado realizasse auditorias dos resultados contábeis das empresas para garantir que as empresas não estavam fraudando o fisco.

7.1.2 Período de 1840 a 1920

Neste período, a atividade de auditoria se expandiu com a Revolução Industrial na Inglaterra, quando começaram a surgir as indústrias e o uso intensivo de capital monetário. Neste período também surge uma classe média, com capital para investimento, em um mercado recém-criado e sem regulação alguma. Nasce a necessidade de verificar o estado contábil das empresas, não somente para detectar fraudes contra o fisco, mas para proteger os investidores.

Começam a aparecer as primeiras legislações sobre auditorias: em 1844, e revisado em 1856, é estipulado o *Joint Stock Companies Act* o qual estipula que “os diretores são responsáveis pelo equilíbrio contabilístico e por demonstrações de resultados completos e justos”, além de serem designados auditores para a verificação de contas destas companhias. Em 1845, também é publicado o *Railway Companies Consolidation Act*, que institui a verificação anual dos balanços, feita por auditores. Neste período, usualmente os auditores eram acionistas escolhidos pelos seus pares (TECK-HEANG et al., 2008).

Com a instituição de auditorias obrigatórias também começa o estudo e criação de metodologias de auditoria, o livro *Auditing: a practical manual for auditors*, escrito por Lawrence Robert Dicksee e publicado em 1892, é um exemplo.

7.1.3 Período de 1920 a 1960

Neste período acontece a expansão dos Estados Unidos da América após a Primeira Guerra Mundial e o polo de desenvolvimento da auditoria é modificado para o novo continente. A percepção da necessidade de auditorias é fortemente influenciada pela crise de 1929. Este período também é marcado

pelo grande desenvolvimento das empresas de seguro e garantidoras de crédito. Empresas que necessitam possuir confiabilidade nas informações apresentadas pelos seus clientes para garantir a continuidade da sua existência.

Soma-se a este fato o crescimento das empresas em tamanho e complexidade, que começam a ter uma separação muito grande entre os donos e os gerentes das empresas. Na década de 30 é criado o comitê *May*, um grupo de trabalho com a finalidade de estabelecer regras para as empresas que tivessem suas ações cotadas em bolsa, tornando obrigatória a execução de auditoria contábil independente nos demonstrativos contábeis das empresas (PINHO, 2007).

No trilhar deste caminho modifica-se o foco das auditorias. Além do estado não ser mais o ente principal interessado nos resultados das auditorias, o objetivo principal não é encontrar fraudes e sim dar credibilidade para os gestores e acionistas das informações contábeis, garantir a eficiência e qualidade do trabalho realizado e também a honestidade e integridade moral dos funcionários.

Outra modificação neste período é a utilização da amostragem para a realização das auditorias. Devido ao crescimento das corporações e o volume das transações realizadas tornou-se impossível auditar a totalidade das transações. Nesta época a auditoria torna-se um negócio rentável e com forte competição entre os grandes escritórios.

7.1.4 Período de 1960 a 1990

A principal marca desta época é o desenvolvimento tecnológico. A utilização dos computadores permitiu o crescimento e a gerência de organizações extremamente complexas. Esta alteração no cenário teve também impacto na prática da auditoria.

Com o advento da criação de sistemas de informação, os auditores modificaram a prática de verificar as transações nos livros – verificando contas e valores – para confiar nos sistemas. Esta alteração é baseada em vários fatores: complexidade das empresas, número de transações e também confiança nos sistemas de informação.

Os auditores começam a modificar a base da auditoria. Não mais cada transação específica, mas os controles internos existentes na empresa. Caso

verificassem que os controles internos da empresa eram efetivos em algumas áreas, diminuíam o interesse nestas e auditavam mais detalhadamente as áreas com controles internos pouco efetivos.

Durante a década de 1980 esta abordagem é fundamentada teoricamente como auditoria baseada em risco, em que os auditores irão escrutinar áreas onde é mais provável a existência de erros. Nesta época também surge uma pergunta importantíssima para o nosso estudo: podemos confiar nos sistemas de informação e seus controles?

7.1.5 Período de 1990 a 2017

A profissão do auditor testemunhou uma grande mudança na época atual. Principalmente a evolução de uma visão extremamente contábil para auditoria em todas as áreas. A definição de auditoria transita de um conceito contábil para o negócio de prover um testemunho de que um cliente é aderente com algum estatuto, lei ou requisito similar (HALL, 2011).

Outra evolução é a abordagem baseada em riscos, a qual solidifica um arcabouço teórico e passa a dominar a atividade da auditoria. Esta abordagem possibilita ao auditor realizar o seu trabalho com relevância e significância respeitando os prazos, pois como já discutido, o tamanho e complexidade das empresas torna impossível examinar todas as transações desta. Entretanto tornou necessária a compreensão dos riscos de negócio da empresa.

Também a perspectiva da análise de riscos modifica-se, parando de considerar somente os riscos financeiros: começa a considerar os riscos para o cliente. Esta mudança de perspectiva é fortemente influenciada pelo estudo da cadeia de valores (PORTER, 1999), o qual considera que impactos negativos ao cliente irão suceder em algum momento como impactos financeiros para a empresa.

No início deste período, também se verifica uma alteração no papel das empresas de auditoria, a maioria passa a lucrar mais com o serviço de consultoria do que exercendo a auditoria. Isto leva a um conflito de interesses e falta da independência entre auditores e auditados, um dos pilares da auditoria. Este fato levou os reguladores e investidores a começarem a questionar se empresas poderiam prestar serviço de auditoria e consultoria conjuntos.

Como resposta, atualmente, a maioria das grandes empresas separaram em companhias diferentes o ramo de auditoria e consultoria.

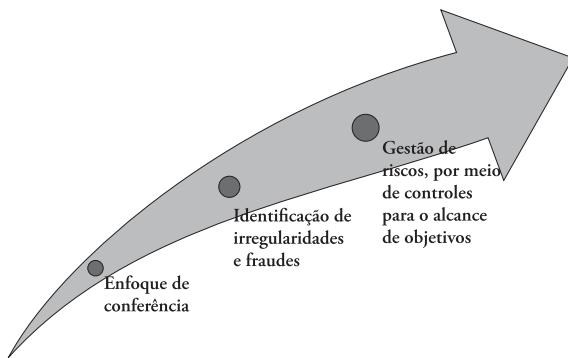
Recentemente, vários eventos no mundo corporativo, novas leis e novas *frameworks* de auditoria forçaram a evolução de como a auditoria é realizada.

- × Modelos COSO I e II (1992 e 2004), em reação à ocorrência de fraudes em relatórios financeiros e contábeis;
- × A Lei *Sarbanes-Oxley* (SOX), uma lei estadunidense assinada em 2002 pelo senador Paul Sarbanes e pelo deputado Michael Oxley. A lei foi motivada por escândalos financeiros corporativos (entre estes, o da Enron, que acabou por afetar drasticamente a empresa de auditoria Arthur Andersen). Esta lei foi redigida com o objetivo de evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores causada pela aparente insegurança a respeito da governança adequada das empresas. É considerada uma das mais rigorosas regulamentações que trata de controles internos, elaboração de relatórios financeiros e divulgações;
- × As recomendações da *International Organization of Supreme Audit Institutions (Intosai)* para adoção de padrões e estruturas de controle interno calcados no gerenciamento de riscos e em modelos de governança corporativa.

7.2 A evolução da auditoria de sistemas de informação

Como é demonstrado na história da auditoria, com a evolução das corporações e do processo de auditoria houve uma mudança na metodologia das auditorias, com a utilização de amostras e também a abordagem de riscos, em que se passou a verificar os controles existentes na empresa. A figura 7.1 demonstra aspectos desta mudança de enfoque:

Figura 7.1 – Evolução do paradigma da auditoria



Fonte: TCU (2011).

Por outro lado, a evolução e a ubiquidade da tecnologia de informação modificaram completamente o cenário corporativo. Cada vez mais a utilização de papel para armazenar informações torna-se uma atividade que será mostrada somente nos museus de história. Além do armazenamento, também foi natural a implantação dos controles internos nos sistemas de informação.

A auditoria depende de dados para criar materialidade das inconformidades e dos controles internos para utilizar a abordagem de riscos. Portanto, a própria auditoria contábil é fortemente influenciada pela confiabilidade dos sistemas da informação. Diante de todas as informações obtidas, chegou-se à conclusão de que o escopo da auditoria está intrinsecamente associado à avaliação dos sistemas informatizados envolvidos, vez que qualquer dado errôneo ou fraudulento necessariamente estará registrado nos sistemas e deixará pistas que podem ser mais facilmente identificadas por especialistas em tecnologia da informação (TCU, 2001).

Frente a esta grande dependência das empresas dos sistemas de informação e crescente complexidade dos ambientes computacionais, os auditores perceberam a necessidade de atrair profissionais capacitados para investigar o funcionamento dos sistemas de informação.

De todo modo, as auditorias nos sistemas de informação vão muito além de verificar somente informações da área contábil. As auditorias atuais verificam se algum sistema de informação está de acordo com algum padrão, seja de segurança, governança ou conformidade com a legislação.

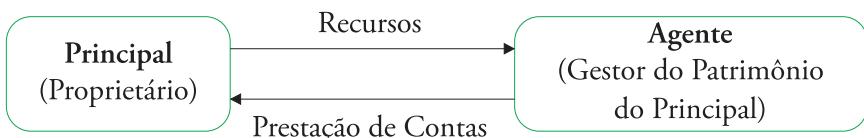
A dependência das empresas tornou os sistemas de informação um item estratégico. A implantação de um sistema novo pode, em alguns casos, alterar completamente o funcionamento de uma organização e até ser a diferença entre o sucesso ou a falha de um projeto. Com a necessidade de auditar os sistemas de informação, começou-se a criar um arcabouço de conhecimento e padrões para os sistemas de informação.

7.3 Objetivos da auditoria

A auditoria torna-se uma atividade importante e necessária ao proprietário que delega um patrimônio para ser gerido por um terceiro. Espera-se que o agente – o gestor – sempre tome ações que sejam no melhor interesse do principal – o proprietário.

Podemos definir esta relação com a teoria da agência. Uma relação de agência é um contrato sob o qual uma ou mais pessoas (os principais) contratam outras pessoas (os agentes) para desempenhar algum serviço que envolva delegação de alguma decisão ao agente. No entanto, muitas vezes ocorre o conflito de interesses e o agente pode tomar decisões em benefício próprio e não em função do proprietário. Este conflito é chamado conflito da agência (JENSEN et al., 1976). A figura 7.2 exemplifica esta relação:

Figura 7.2 – Relação entre principal e agente



Fonte: Elaborada pelo autor.

A auditoria serve como um instrumento de governança no intuito de verificar se os interesses do principal estão sendo atendidos e se, ao delegar a gestão dos seus recursos, o agente não está utilizando estes recursos para si

mesmo. O motivo dos agentes não trabalharem para os melhores interesses do principal podem ser de dois tipos:

- ✖ objetivo – decorrente da deficiência administrativa, ausência ou insuficiência de controles internos;
- ✖ subjetivo – quando o gestor por negligência, imprudência ou imprecície deixa de tomar uma ação.

Conceptualmente, a auditoria de sistemas de informação é o processo de assegurar se o desenvolvimento, implantação e manutenção de sistemas atingem os objetivos de negócio, segurança dos itens de informação e mantém a integridade dos dados. Em outras palavras, auditoria de sistemas de informação é uma avaliação da implantação dos sistemas de controles para assegurar que os sistemas atingem as necessidades do negócio sem comprometer a segurança, privacidade, custo e outros elementos críticos do negócio (IMONIANA, 2016).

A auditoria de sistemas de informação busca avaliar se os sistemas, práticas e operações podem incluir:

- ✖ uso dos controles internos dentro do ambiente de sistemas de informação para assegurar validade, confiabilidade e segurança da informação;
- ✖ eficiência e efetividade dos sistemas de informações em termos econômicos.

Os critérios listados anteriormente estão fortemente relacionados aos critérios de informações do COBIT, os quais são:

- ✖ confidencialidade;
- ✖ integridade;
- ✖ disponibilidade;
- ✖ eficácia;
- ✖ eficiência;
- ✖ conformidade;
- ✖ confiança.

Inconformidades nos critérios anteriores podem se manifestar de modo isolado ou conjunto em uma informação. Durante a auditoria, será verificado se estes critérios são aplicados uniformemente nos sistemas e subsistemas.

7.4 Conceitos

Em termos amplos, o conceito para auditoria segundo o Tribunal de Contas da União é “o exame independente e objetivo de uma situação ou condição, em confronto com um critério ou padrão preestabelecido, para que se possa opinar ou comentar a respeito para um destinatário predeterminado” (TCU, 2011). A seguir, listamos alguns conceitos complementares relacionados à auditoria.

- × **Exame independente e objetivo:** a auditoria deve ser realizada por pessoas com independência em relação ao seu objeto, de modo a assegurar imparcialidade no julgamento. O exame objetivo significa que os fatos devem ser avaliados com a mente livre de vieses, de modo a conduzir a julgamentos imparciais, precisos e a preservar a confiança no trabalho do auditor.
- × **Situação ou condição:** é a condição ou o estado do objeto de auditoria encontrado pelo auditor. Comumente denominada situação encontrada, representa o que está ocorrendo, é o fato concreto.
- × **Critério ou padrão preestabelecido:** configura a situação ideal, o grau ou nível de excelência, de desempenho, qualidade e demais expectativas preestabelecidas em relação ao objeto da auditoria; é o que deveria ser ou o que deveria estar ocorrendo.
- × **Opinião ou comentário:** refere-se à comunicação dos resultados da auditoria, seu produto final. Expressa a extensão na qual o critério ou padrão preestabelecido foi ou está sendo atendido.
- × **Destinatário predeterminado:** é o cliente da auditoria. É aquele que, na grande maioria das vezes, estabelece o objetivo da auditoria e determina os seus critérios ou padrões.

Como foi apresentado no histórico, os conceitos, práticas e todo um arcabouço relacionado ao mundo da auditoria sofreram evolução durante os anos

até chegar ao estado atual, sendo que esta evolução é extremamente ligada ao aumento em tamanho e complexidade das corporações. A auditoria não está mais relacionada apenas ao governo, confinada à tarefa de revelar e detalhar fraudes das entidades com o dinheiro público. O foco agora é auditar se as organizações apresentam uma boa gestão, verificando os controles internos existentes e a aderência às melhores práticas gerenciais nos órgãos fiscalizados. Mesmo os órgãos governamentais de auditoria, como o TCU no Brasil, procuram não só encontrar fraudes, mas verificar se os órgãos são bem gerenciados.

Para fundamentar a auditoria de sistemas de informação e apresentar as metodologias dessa auditoria – assunto discutido no próximo capítulo – vamos evoluir para os conceitos e princípios essenciais para a execução de uma auditoria.

7.4.1 Controle Interno

Controles internos são planos organizacionais e coordenação de um conjunto de métodos e medidas adotadas em uma empresa, a fim de salvaguardar o ativo, verificar a exatidão e veracidade de registros contábeis, promover a efetividade de sistemas de informação contábil e eficiência operacional, assim como fomentar uma grande adesão às políticas da organização.

A utilização de um controle pode estar ou não dentro de um sistema de informação, o importante é a existência deste controle, garantindo a qualidade final das atividades. Podemos listar quatro tipos de atividades de controle, descritas a seguir.

- × **Preventivo:** são controles projetados para prevenir a ocorrência de erros, ineficácia e irregularidades. Estes controles não garantem que a erradicação destes itens irá ocorrer, mas diminuem a probabilidade. Alguns exemplos destes controles são: segregação das funções e aprovação de tarefas;
- × **Diretivo:** são controles para encorajar eventos e alcançar objetivos e metas da empresa. Exemplos incluem a definição de políticas, procedimentos e treinamentos adequados da equipe.
- × **Corretivo:** identificar e avaliar cursos alternativos de ação para avaliar medidas apropriadas para consertar situações e minimizar

danos. Exemplos: correção de erros durante cálculo computacional; validação na entrada de dados.

- × **Detecção:** controles para detectar e corrigir erros. Estes controles atuam depois da execução de uma operação, portanto, também depois da ocorrência do erro. Exemplos: verificação do saldo bancário após uma transferência; verificação de estoque após o lançamento de uma alteração.

Os controles internos existentes devem ser comunicados aos colaboradores e também devem ser valorizados. Por exemplo, a segregação de funções pode ser prejudicada quando informalmente os colaboradores passam a confiar completamente em um colaborador. Ou o controle de acesso, a senha por exemplo, passa a ser compartilhada pelos usuários. Isso pode levar à falha do controle interno.

7.4.2 Risco

A avaliação de risco é essencial para a auditoria moderna. Com a complexidade das organizações e quantidade de transações, não é possível auditar todas as áreas e transações de uma organização. Portanto, é utilizada uma amostra para auditoria. A questão é como escolher esta amostra. Esta escolha é baseada nas amostras de maiores riscos da auditoria. São escolhidos itens com o intuito de mitigá-los. Costuma-se medir o risco pelas seguintes dimensões: impacto do risco, e probabilidade do risco acontecer. A figura 7.3 apresenta um exemplo de matriz de risco.

Figura 7.3 – Matriz de Risco

	4 – Alto	4	8	12	16
	3 – Significativo	3	6	9	12
	2 – Moderado	2	4	6	8
	1 – Baixo	1	2	3	4
Impacto		1 – Remota	2 – Improvável	3 – Possível	4 – Provável
	Probabilidade				

Fonte: Elaborada pelo autor.

Podemos utilizar esta matriz de risco da seguinte maneira: Qual o risco de um disco do computador pessoal do presidente, onde estão armazenados

vários arquivos gerenciais, sem backup em outras máquinas, falhar nos próximos 2 anos?

Avaliando os atributos do HD utilizado no computador da presidência, pode-se verificar que existe a possibilidade do HD vir a falhar, portanto, a probabilidade do risco pode ser atribuída o valor de Possível. Já o impacto da perda dos arquivos armazenados no computador pessoal do presidente, sem backup destes arquivos, pode ser visto como alto, pois serão perdidas informações importantes para o gerenciamento da empresa. Portanto, na matriz de risco o valor do risco seria 12. Esta classificação é muito útil para comparar riscos diferentes.

A figura 7.4 apresenta o cálculo do risco de um disco no computador pessoal do presidente da empresa, onde estão armazenados vários arquivos gerenciais, sem backup em outras máquinas falhar nos próximos 2 anos.

Figura 7.4 – Exemplo de cálculo de risco

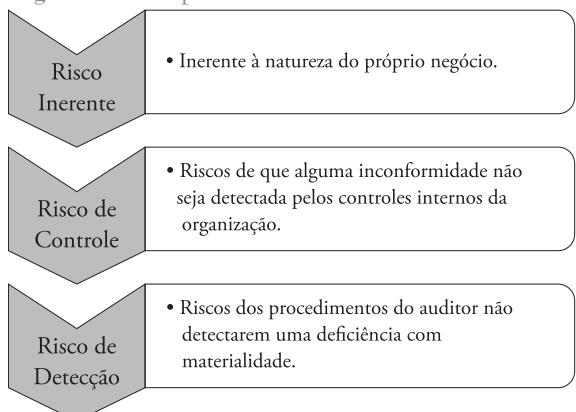
Impacto	4 – Alto	4	8	12	16
	3 – Significativo	3	6	9	12
	2 – Moderado	2	4	6	8
	1 – Baixo	1	2	3	4
	1 – Remota	2 – Improvável	3 – Possível	4 – Provável	
	Probabilidade				

Fonte: Elaborada pelo autor.

O cálculo de risco da auditoria deve considerar a junção de três tipos de riscos: o risco inerente, o risco de controle e o risco de detecção. A figura 7.5 apresenta estes três tipos:

- ✗ O **risco inerente** pode ser definido como o risco do próprio

Figura 7.5 – Tipos de riscos



Fonte: Elaborada pelo autor.

negócio, influenciado pela sua natureza, portanto áreas diferentes de atuação possuem riscos diferentes. Por exemplo, um software de controle de voo tem um risco muito maior – pois o impacto de qualquer problema é muito grande – quando comparamos com o risco de um sistema de controle de pedágio.

- ✗ O **risco de controle** está relacionado à existência de erros materiais, que não sejam detectados ou previstos pelos controles internos da organização. Devido à própria natureza e custo dos controles internos é improvável que um controle interno evite totalmente o risco de uma inconformidade.
- ✗ O **risco de detecção** é o risco existente de os procedimentos realizados pelo auditor não detectarem uma deficiência com materialidade nos sistemas de informação.

O risco da auditoria é a junção dos três riscos:

- ✗ **Risco da Auditoria** = Risco Inerente ✗ Risco de Controle ✗ Risco de Detecção

Os riscos estão relacionados à natureza da organização e também aos processos e controles internos da empresa. Portanto, para calcular os riscos é necessário que o auditor tenha conhecimento da empresa, incluindo pessoas responsáveis pelas atividades, comprometimento do pessoal envolvido, processos e controles internos.

7.4.3 Tipos de auditoria

Existem dois tipos de auditoria: **externa** e **interna**. A auditoria externa diferencia-se principalmente por ser realizada por uma organização independente e externa de auditoria, com o uso de um arcabouço específico. A auditoria externa busca o maior grau possível de independência com a empresa auditada.

A auditoria interna, por sua vez, diz respeito ao vínculo mantido entre o auditor e a entidade auditada. Em uma auditoria interna a unidade da auditoria integra a estrutura da organização. Diferencia-se por ter como foco auxiliar os gestores a alcançar os objetivos da empresa. A auditoria interna é uma atividade independente, de garantia e de consultoria, destinada a acrescentar

valor e a melhorar as operações de uma organização. Assiste à organização na consecução dos seus objetivos, por meio de uma abordagem sistemática e disciplinada, para a avaliação e melhoria da eficácia dos processos de gestão de risco, controle e governação (IIA, 2013).

A auditora interna é realizada por empregados da própria empresa. De todo modo, ainda é observado um alto grau de independência para auditores. Para garantir esta independência, usualmente os auditores estão submetidos hierarquicamente diretamente aos acionistas ou ao CEO da empresa.

As informações da auditora vão auxiliar e direcionar a tomada de decisões dos gestores. A auditoria interna busca examinar e avaliar a qualidade dos controles.

7.5 Auditor – perfil e ética

A ética é o conjunto de normas que orienta a conduta de determinada categoria. O devido zelo e a observância de padrões de conduta profissionais devem ser observados durante a execução da auditoria. O código de ética da IIA (IIA, 2009) apresenta quatro princípios que devem reger a ética do auditor: integridade, objetividade, confidencialidade e competência.

Um auditor deve ter a integridade como característica. Sempre ser honesto e imparcial em seus julgamentos, mantendo sempre a objetividade, efetuando uma avaliação equilibrada de todas as circunstâncias relevantes, e não indevidamente influenciado pelos interesses próprios ou de terceiros. Deve prestar os esclarecimentos necessários para que os interessados na auditoria compreendam o resultado.

Além disso, o auditor também deve servir aos interesses do contratante e partes envolvidas de uma maneira objetiva e condizente com a legislação vigente, mantendo um grande padrão de conduta e caráter, lembrando que seu trabalho poderá ter resultado não somente na empresa, mas também na sociedade.

O auditor de sistemas de informação, durante a execução do seu trabalho, terá acesso a informações sigilosas sobre a empresa. Algumas vezes serão informações internas que são desconhecidas pelos próprios colabora-

dores. Estas informações devem ser repassadas somente aos canais competentes, pois poderiam ser utilizadas pela concorrência ou até para política interna da empresa. Portanto, é imprescindível para um auditor saber o que e a quem comunicar.

Por último, o auditor deve comprometer-se a auditar somente os serviços os quais ele tem conhecimentos, habilidades e experiências necessários para a realização do trabalho.

A ISACA também mantém um código de ética (ISACA, 2010), o qual serve como um balizador para as ações do auditor. Para associados que desrespeitam este código, as ações podem resultar em investigação e medidas disciplinares. O código de ética da ISACA é composto de sete itens:

1. respeito à implementação, e promover o cumprimento com os padrões e procedimentos apropriados de governança e gestão efetiva dos sistemas de informação e tecnologia da empresa, incluindo gestão de auditoria, controle, segurança e riscos.
2. realizar os trabalhos com objetividade, diligência e rigor/cuidado profissional, de acordo com os padrões profissionais.
3. servir em benefício das partes interessadas de um modo legal e honesto e, ao mesmo tempo, manter altos níveis de conduta e caráter, e não participar de atos que desacreditem sua profissão ou associação.
4. manter a privacidade e confidencialidade da informação obtida no curso dos seus deveres. A informação não deve ser utilizada para benefícios pessoais.
5. manter a aptidão nos seus respectivos campos e assumir somente aquelas atividades que tem habilidade, conhecimento e competência necessários.
6. informar o trabalho realizado às partes apropriadas, incluindo a revelação de todos os atos significativos.
7. respeitar a educação profissional das partes interessadas para que tenham a melhor compreensão da governança e gestão dos sistemas de informação e tecnologia da empresa.

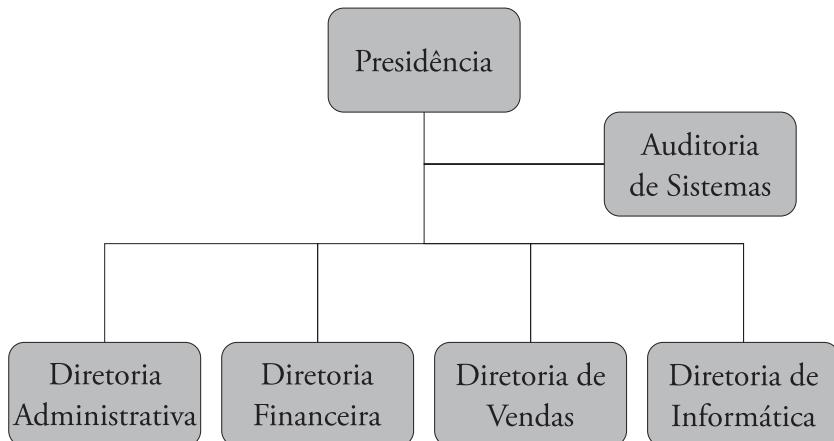
Como é possível visualizar, o código de ética da ISACA e da IIA são compatíveis entre si, não há nenhum conflito em seus princípios.

7.5.1 Independência profissional

O auditor deve manter independência em relação à empresa ou ao setor auditado. Esta independência visa estabelecer a imparcialidade de auditor, permitindo uma conclusão objetiva da auditoria, livre de condições que ameacem seu resultado.

Esta independência deve ser resguardada individualmente por cada auditor, além de ser resguardada pela empresa funcional e hierarquicamente. Portanto, deve ser observada pelo profissional, mas também gestores, ao conceder aos auditores internos acesso à gerência sênior, evitando pressões para modificação de relatórios ou pareceres. A figura 7.6 apresenta um organograma sugerido para o setor de auditoria interna, evitando que relacionamentos hierárquicos venham a afetar o resultado da auditoria.

Figura 7.6 – Organograma sugerido para o setor de auditoria interna



Fonte: Elaborada pelo autor.

Pelo código de ética profissional, um auditor, externo ou interno, também não pode executar auditoria de parentes, preservando a objetividade e independência da auditoria.

7.5.2 Competência

Os novos paradigmas da auditoria modificaram muito a atuação e o perfil necessários do auditor. De simples conferidor de transações contábeis, tornou-se necessário conhecer os modelos de gestão e governança. O alinhamento dos sistemas de informação com a visão da estratégia e objetivos da empresa são considerados durante a auditoria. Alguns autores começaram a visualizar a necessidade dos auditores terem a visão de homens de negócio. “Os auditores terão que ser melhores homens de negócio; inclusive, terão que ser, primeiro, bons homens de negócio e, em segundo lugar, bons auditores” (TCU, 2011, p. 22, apud CASTANHEIRAS, 2007).

O auditor de sistemas de informação, além das competências necessárias para um auditor, deverá também ter as habilidades e conhecimentos necessários em tecnologia para a execução da auditoria. Portanto, é necessário constante aprendizado, condizente com os avanços tecnológicos da área de TI.

Segue uma lista de conhecimentos necessários para o trabalho de auditor:

- × conceitos de tecnologia da informação
- × fundamentos de arquitetura de sistemas;
- × rede de computadores;
- × programação de computadores;
- × linguagens de modelagem: UML, ER etc.;
- × gerenciamento de riscos, privacidade, desenvolvimento e implantação de políticas e estratégias de segurança de informações;
- × iniciação de trilha de auditoria em ambiente de tecnologia de informação e propriedade intelectual;
- × softwares de auditoria.

Deste modo, a formação continuada é necessidade de um auditor, pois sempre haverá novos arcabouços de governança, modelos de gestão e novas tecnologias.

7.6 Empresas de auditoria externa e consultoria

No início dos anos 90, utilizando os paradigmas modernos de auditoria, as empresas de auditoria apontavam problemas, fossem contábeis, ou nos controles de sistemas de informação nas empresas em relação aos melhores modelos de gestão e padrões do mercado. Neste período, o conhecimento sobre estes controles ainda era escasso no mercado, logo as empresas começaram a fazer contratos de consultoria com as empresas de auditoria.

Em um curto período de tempo, algumas empresas de auditoria começaram a lucrar mais prestando serviço de consultoria, ou seja, mostrando às empresas como elas deveriam funcionar, do que realizando auditorias. Entretanto, este fato começou a afetar a independência das empresas. Por exemplo, uma empresa X paga a empresa A por uma consultoria e gasta dinheiro e esforço para conseguir executar as mudanças propostas pela empresa A. Passados alguns meses, a mesma empresa A vem auditar esta empresa X. Qualquer crítica ao funcionamento da empresa X será também uma crítica à consultoria executada pela própria empresa A.

Isto afetou profundamente a independência das empresas de auditoria, pois estas não eram mais totalmente independentes na emissão do parecer. Este fato foi tão relevante que as grandes empresas envolvidas nestes contratos tiveram de dividir as empresas, uma especializada em auditoria e outra em consultoria.

7.7 Planejamento

O primeiro passo antes de executar qualquer auditoria é o planejamento. Este planejamento deve considerar quais são os objetivos da auditoria, considerando as normas éticas e leis aplicáveis ela.

Como discutido, na abordagem baseada em riscos o auditor deve detalhar a auditoria, baseado na probabilidade de encontrar inconformidades. Deste modo, é necessário conhecimento das estruturas, relações e controles

internos da empresa. Estas escolhas devem ser documentadas, para caso seja necessário, ser possível recuperar a informação.

O auditor deve desenvolver o plano de auditoria detalhando a natureza, época e extensão dos procedimentos da auditoria necessários para sua conclusão. Este plano não é estático, pode ser modificado durante a execução da auditoria devido a novos achados ou suposições que foram feitos incorretamente na fase de planejamento.

7.8 Relatório

A contratação de um serviço de auditoria com uma firma de auditoria independente, busca uma opinião sobre a adequação de políticas e procedimentos de um serviço da organização. Em alguns casos, a auditoria independente pode também verificar se as políticas e procedimentos estão operando de modo efetivo dentro da organização.

O relatório é o produto final do processo de auditoria. É o instrumento formal e técnico por intermédio do qual a equipe de auditoria comunica: o objetivo e as questões de auditoria; a metodologia utilizada; os achados de auditoria; as conclusões; e as propostas de encaminhamento (TRIBUNAL DE CONTAS DA UNIÃO, 2011).

7.9 Ferramentas de Auditoria

Assim como todas as outras atividades foram influenciadas pelo avanço da tecnologia, a própria execução da auditoria foi influenciada pelo avanço da tecnologia da informação.

Mais recentemente, o mercado ganhou diversos softwares que auxiliam nas atividades de auditoria, dispondo de funcionalidades, tais como: gerenciamento do processo de planejamento das atividades de auditoria, contemplando o registro de todas as etapas do trabalho; bancos de dados; programas que promovem o cruzamento de grande volume de informações; e softwares estatísticos. A auditoria dos sistemas de informação também utiliza ferramentas especializadas em analisar código-fonte, segurança dos sistemas e outras atividades. O Tribunal de Contas da União classifica as ferramentas de apoio à auditoria nos seguintes tipos:

- ✖ **softwares de processamento de dados** – para estruturação de dados, tratamento de dados, cruzamento de informações. Exemplos: Access (banco de dados), Excel (planilhas, gráficos), ACL (cruzamento de dados de fontes independentes).
- ✖ **softwares estatísticos** – fazem análises estatísticas, amostragens estatísticas, inferências de determinadas situações para um conjunto de operações. Exemplos: SPSS, SAS.
- ✖ **ferramentas de gerenciamento e execução** – são necessárias ferramentas para o registro e acompanhamento das fases de planejamento e execução das auditorias; registro das equipes designadas às atividades de fiscalização em determinado momento, mês ou ano; registro das recomendações e determinações para efeito de monitoramento ou *follow-up* dessas deliberações junto às organizações auditadas. Algumas ferramentas conhecidas: *TeamMate*, *Fiscalis*, e-TCU.
- ✖ **sistema de documentação** – criação de padrões de armazenamento e acesso às informações; definição de uma estrutura padrão para os relatórios de auditoria, com base em modelo reconhecidamente de boa aceitação, principalmente dos clientes e público-alvo; implementação de regras e mecanismos que auxiliem no controle de qualidade do trabalho; auxílio no alinhamento das ações e práticas realizadas às normas de auditoria que regam o exercício dessa atividade.
- ✖ **ferramentas de produtividade** – implantação de rotinas e procedimentos que favoreçam a efetiva gestão do conhecimento internamente à unidade de auditoria; criação e manutenção de uma ativa “biblioteca dos trabalhos de auditoria”, contemplando, entre outros, os registros dos trabalhos já realizados, procedimentos de auditoria padrão etc.; mecanismos de geração automática de relatórios, e de trabalho em grupo (chat, vídeo e teleconferência etc.); dispositivos off-line para os trabalhos em campo, que permitem o registro, fora do domicílio, dos procedimentos realizados, matrizes e relatórios, com posterior integração e armazenamento desses dados via internet ou rede interna;
- ✖ **ferramentas de avaliação de riscos** – adoção de ferramentas que automatizem e facilitem os cálculos, ponderações e análises para

efeito de avaliação do risco de auditoria; criação de matrizes de risco, ou metodologia científica (matemática e/ou estatística) que cumpram essa função e que permitam, por outro lado, a flexibilidade de inserção, a qualquer tempo, de novos fatores e aspectos subjetivos que devam ser considerados no modelo de avaliação de risco adotado; emissão de relatórios gerenciais para suporte à tomada de decisão nos níveis estratégicos.

7.10 Associações e certificações

As associações e seus padrões buscam um conjunto de procedimentos-modelo para a atividade de auditoria. Para o profissional de auditoria, ter uma certificação e ser membro de uma dessas associações dará credibilidade para o produto do seu trabalho.

Existem várias associações de auditoria, cada uma delas tem um foco específico, com os próprios padrões e certificações. Ao ganharmos conhecimento nos vários padrões existentes, iremos verificar a existência de uma grande conexão no conhecimento que há em cada um deles. Compreender a conexão entre cada uma destes padrões é dever de um bom auditor.

No quadro 7.1 é possível visualizar as associações, certificações e padrões importantes para a profissão do auditor de sistemas de informação. Esta lista não é exaustiva e existem várias associações, certificações e padrões disponíveis no mercado. Os padrões COBIT e ISO 27001 já foram abordados no capítulo 2 e por isso não serão discutidos novamente.

Quadro 7.1 – Associações, certificações e padrões

Associação	Certificações	Padrões
ISACA	CISA, CISM, CGEIT, CRISC, COBIT	COSO, COBIT
INTOSAI	-	ISSAI
IIA	CIA, CCSA, CFSI, CGAP, CRMA	-

Associação	Certificações	Padrões
ISO	ISO 27001 – Auditor Líder	ISO 27001

Fonte: Elaborada pelo autor.

A seguir elencamos um resumo das principais associações e certificações existentes atualmente:

7.10.1 Information System Audit and Control Association – ISACA

Acrônimo para *Information System Audit and Control Association* (Associação de Auditoria e Controle de Sistemas de Informação). Auxilia profissionais em todo o mundo atuando no desenvolvimento de metodologias e certificações. A ISACA foi fundada em 1969, sendo uma associação global sem fins lucrativos com 140 mil profissionais em 180 países. Algumas das certificações profissionais da ISACA com alto reconhecimento no mercado:

- × **CISA** – Certified Information Systems Auditor;
- × **CISM** – Certified Information Security Manager;
- × **CGEIT** – Certified in the Governance of Enterprise IT;
- × **CRISC** – Certified in Risk and Information Systems Control.

7.10.2 Certified Information System Auditor – CISA

Certificação concedida pela ISACA. Tem reconhecimento mundial como um padrão para a realização de auditoria, controle, monitoramento e avaliação de sistemas de informação e negócios nas organizações. Atualmente é uma das certificações mais importantes para auditores na área de tecnologia de informação. A designação CISA reconhece profissionais que demonstraram experiência, habilidades e conhecimento para auditar sistemas de informação, considerando:

- × o processo de auditoria de sistemas de informação;

- × a estrutura e processos de governança e gestão de TI;
- × o processo de aquisição, desenvolvimento e implementação de sistemas de informação;
- × a operação, manutenção e suporte a sistemas de informação;
- × a proteção de ativos de informação (políticas, normas, procedimentos e controles).

7.10.3 The Institute of Internal Auditors – IIA

Esta associação tem o foco no desenvolvimento da profissão dos auditores internos. Criada em 1941 na Flórida, Estados Unidos da América. Seus membros usualmente atuam na área de auditoria, gerenciamento de riscos, governança, controle interno, auditoria de tecnologia de informação, educação e segurança. Tem mais de 185 mil membros no mundo. As certificações da IIA incluem:

- × CIA – Certified Internal Auditor;
- × CCSA – Certification in Control Self-Assessment;
- × CFS – Certified Financial Services Auditor;
- × CGAP – Certified Government Auditing Professional;
- × CRMA – Certification in Risk Management Assurance.

7.10.4 Certified Internal Auditor – CIA

Certificação primária oferecida pela IIA. A CIA é reconhecida mundialmente como uma certificação para auditores internos. De acordo com a própria IIA, esta certificação tem como objetivo:

- × dar credibilidade perante a equipe interna e os clientes externos;
- × desenvolver conhecimento sobre as melhores práticas no setor;
- × estabelecer uma base para melhoria contínua e aprimoramento.

Para ser elegível para uma certificação CIA o profissional deverá ter formação e experiência profissional comprovada, conforme quadro 7.2:

Quadro 7.2 – Formação e experiência comprovada para certificação CIA

Formação	Experiência
Diploma de bacharel	Dois anos de experiência comprovados
Cursos tecnológicos (2 anos)	Cinco anos de experiência comprovados
Sem curso superior	Sete anos de experiência comprovados

Fonte: Elaborada pelo autor.

7.10.5 International Organization of Supreme Audit Institutions – INTOSAI

Organização Internacional de Entidades Fiscalizadoras Superiores (INTOSAI). As entidades fiscalizadoras superiores são entidades governamentais de auditoria, como por exemplo o Tribunal de Contas da União no Brasil.

É uma organização não-governamental, autônoma, independente e apolítica, fundada em 1953, com status consultivo especial no Conselho Econômico e Social das Nações Unidas e trabalha no sentido de promover o intercâmbio de informações e de experiências sobre os principais desafios enfrentados pelas entidades fiscalizadoras superiores de vários países no desempenho de suas funções.

Síntese

Neste capítulo foi apresentada a auditoria de sistemas de informações, com introdução de seus conceitos básicos, histórico e o perfil do profissional desta área. Além disso, foi demonstrada a evolução da auditoria durante as épocas, incluindo as motivações e mudanças que levaram a auditoria de sistemas de informação ao paradigma atual.

Um ponto importante deste capítulo é a apresentação de como a auditoria atual utiliza a gestão de riscos, por meios de controles, para alcançar

um bom resultado. Compreender e atuar sobre este paradigma, utilizando os conceitos de auditoria de sistemas de informação, sejam eles gerenciais, técnicos ou éticos são essenciais para o profissional de auditoria de sistemas de informação. Por último, foram listadas algumas associações e a importância delas para o trabalho do auditor de sistemas de informação.

Atividade

1. Defina a teoria da agência e discuta sua importância para a auditoria.
2. Qual a importância da amostragem para a auditoria moderna? Discuta se utilizar amostragem na auditoria aumenta seu risco.
3. Defina controle interno. Qual o impacto de bons controles internos na auditoria, considerando que o auditor está realizando uma auditoria com análise de risco?
4. Quais são os riscos envolvidos na auditoria? Defina cada um deles.

8

Metodologia de Auditoria de Sistemas de Informação

APÓS TEREM SIDO apresentados os fundamentos da auditoria de sistemas de informação no capítulo anterior, o próximo passo é compreender qual o caminho para executar uma auditoria de sistemas de informação. Este será o foco do capítulo: métodos e processos para a realização de uma auditoria de sistemas de informação.

É IMPORTANTE AFIRMAR que não existe um único método ou técnica para a realização de uma auditoria de sistemas de informação. A metodologia sempre dependerá da abrangência, objetivo e alvo da auditoria. Uma auditoria realizada por uma Entidade Fiscalizadora Superior (EFS) – como o TCU no Brasil – seguirá uma metodologia diferente de uma auditoria contratada por uma empresa após a compra de um sistema de informação. Entretanto, existem algumas fases comuns a todas auditorias.

NESTE CAPÍTULO SERÃO abordados alguns destes métodos de auditoria de maneira resumida. As abordagens discutidas neste capítulo estão descritas em documentos com algumas centenas de páginas, portanto seria impossível apresentá-las em um único capítulo.

Objetivo de aprendizagem:

- × Compreender as etapas de um processo de auditoria dentro de uma metodologia praticada atualmente.

8.1 Metodologia, método e técnica

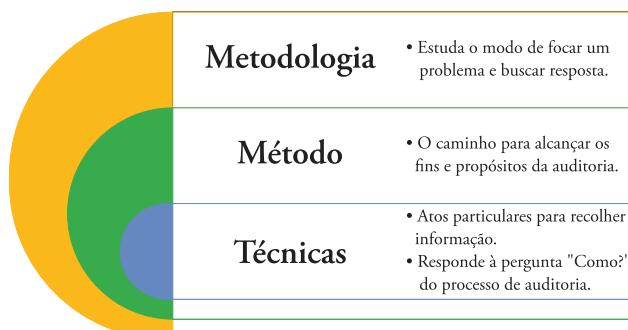
Nos próximos dois capítulos serão estudados métodos e técnicas de Auditoria de Sistemas de Informação, portanto é importante compreender qual a diferença entre metodologia, método e técnica.

A palavra *metodologia* deriva da junção de duas palavras, *método* + *logos*, significando “o estudo dos métodos”. Portanto, a metodologia é a explicação detalhada, rigorosa e precisa de toda ação desenvolvida no método de trabalho.

O método (do Grego *methodos*, *met' hodos* que significa, literalmente, “caminho para chegar a um fim”) é um processo lógico, sistemático e organizado de pesquisa que irá levar ao objetivo pretendido.

A técnica é composta por procedimentos operatórios rigorosos, ligados a uma arte ou ciência, definidos, transmissíveis, susceptíveis de serem novamente aplicados nas mesmas condições, adaptados ao tipo de problema e aos fenômenos em causa. A escolha das técnicas depende do objetivo que se quer atingir, o qual está ligado ao método. A figura 8.1 exemplifica melhor estas diferenças de conceitos:

Figura 8.1 – Relação entre metodologia, método e técnicas



Fonte: Elaborada pelo autor.

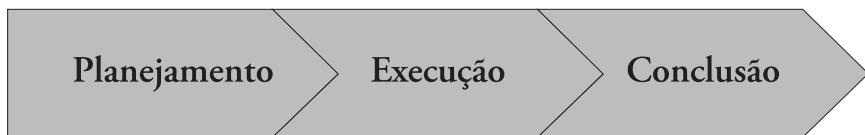
Neste capítulo, portanto, estudaremos os diferentes modos para planejar e executar auditorias. Para alcançar este objetivo, iremos mostrar diferentes métodos, consagrados pela academia e utilizados no mercado para execução de auditorias de sistemas de informação, sejam internos, externos ou governamentais.

8.2 Abordagens de auditoria de sistemas de informação

Apesar de vários métodos de auditoria, cada um com os seus papéis e processos, existem alguns itens comuns a diferentes abordagens (ARIMA, 1993). Para compreender, vamos enumerar diferentes abordagens e suas etapas, incluindo: TCU, fortemente influenciada pela INTOSAI, padrões ISO e IIA.

Sobre as etapas de processo, de uma maneira geral todas as abordagens terão três fases: planejamento, execução e conclusão (vide figura 8.2). Apesar dos nomes diferentes ou subdivisões, estas três etapas estarão presentes. Algumas vezes estarão subdivididas, tendo portanto maiores detalhes. Este detalhamento é bastante influenciado pelo tipo e objetivo da auditoria. Por isso é importante conhecer várias abordagens, para saber utilizar a abordagem correta em cada situação.

Figura 8.2 – Fases padrão de uma auditoria de sistemas de informação



Fonte: Elaborada pelo autor.

8.2.1 IPPF – IIA

O Instituto de Auditores Internos (IIA) tem como objetivo auxiliar os auditores internos em suas atividades, portanto este tipo de auditoria é o foco desta instituição. A organização publicou o *International Standards for the Professional Practice of Internal Auditing* (IPPF), além de alguns guias para abordagens específicas como o *Managing and Auditing IT Vulnerabilities* e o

Developing the IT Audit Plan. Estes guias são norteadores para o trabalho dos auditores internos.

De acordo com o manual (IIA, 1998), de um modo geral todas as auditorias internas vão ser compostas por três grandes etapas: planejamento, execução e relatório. O auditor interno deve estabelecer o que será auditado, assegurar que o plano aprovado será executado e comunicar os resultados alcançados. Além do processo, o IIA lista vários padrões que uma auditoria interna deve possuir, o respeito a estes padrões garante a boa qualidade e credibilidade de uma auditoria interna.

O IPPF tem muito cuidado em mostrar a necessidade de que o auditor seja proficiente nos assuntos necessários a auditoria de sistemas de informação. Em algumas auditorias pode ser necessário que o auditor obtenha novos conhecimentos, dependendo do domínio abordado pelo sistema de informação. Por exemplo, para realizar uma auditoria de um sistema de informação de uma casa de câmbio, será necessário conhecimento da legislação nacional e internacional, além dos processos e boas práticas específicas deste negócio.

O IPPF, como a maioria dos métodos de auditoria moderna, utilizará uma abordagem baseada em riscos.

8.2.1.1 Papéis

O IPPF (RICHARDS et al., 2005) define alguns papéis, responsabilidades e interfaces. A definição dos relacionamentos existentes entre gerência, comitê de auditoria e auditores de TI e a função destes papéis, demonstra a busca pela independência e eficiência da auditoria pelo IPPF.

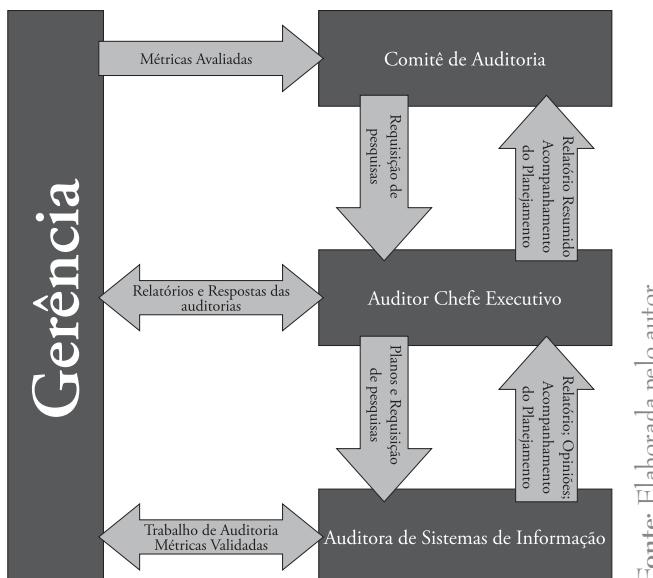
O **comitê de auditoria** faz o papel de representar a vontade dos acionistas da empresa. As responsabilidades deste comitê foram amplamente influenciadas pela SOX (Lei Sarbanes-Oxley), assim como vários dos padrões presentes na IPPF. Este comitê é responsável frente à gerência por proteger os investidores e acionistas. Como estudado na teoria da agência, o comitê de auditoria representa os interesses dos acionistas – o principal – assegurando que as ações e decisões da gerência – o agente – estão sendo feitas, sempre buscando os melhores interesses dos acionistas e respeitando a legislação existente. O comitê de auditoria deve também opinar sobre a contratação e destituição dos auditores.

A IPPF descreve na norma de desempenho 2000 que o auditor chefe executivo é responsável por gerenciar de forma eficaz a atividade de auditoria interna para assegurar que ela adiciona valor à organização. É também seu dever assegurar que os recursos são apropriados, suficientes e efetivamente utilizados para realizar o plano de auditoria aprovado. Deve deter um conhecimento sobre o negócio e os controles internos existentes na empresa, mas não é obrigado a conhecer todas as tecnologias existentes dentro da empresa.

É também dever do auditor chefe executivo o plano de auditoria. Neste plano deverão estar especificados os objetivos específicos, escopo e critérios da auditoria, assegurando que adicione valor para a organização. O plano deverá especificar o que será auditado, o porquê e como será auditado.

O conhecimento específico e técnico é responsabilidade da equipe de auditoria, a qual deve ser composta por auditores experientes e certificados. A equipe de auditores deve ser capaz de coletar dados de modo que os relatórios e opiniões apresentados ao auditor chefe executivo sejam fundamentados. A figura 8.3 resume os relacionamentos entre todos estes entes.

Figura 8.3 – Interfaces entre gerência, comitê de auditoria, auditor chefe executivo e auditores

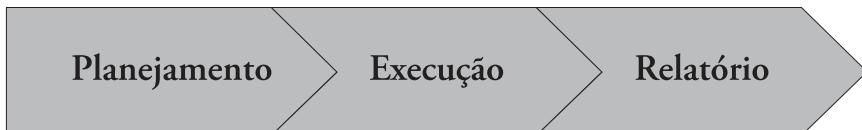


Fonte: Elaborada pelo autor.

8.2.1.2 Etapas

O IIA sugere uma abordagem em três etapas para a execução da auditoria, conforme figura 8.4:

Figura 8.4 – Etapas da auditoria



Fonte: Elaborada pelo autor.

- × Planejamento

A primeira fase da auditoria de sistemas de informação segundo o IPPF é o planejamento. Para a execução do planejamento, é primordial estar definido o enfoque, a abrangência e a delimitação dos sistemas que participarão da auditoria de sistemas de informação. O planejamento da auditoria interna deve ser priorizado considerando os seguintes critérios:

- × datas e resultados das últimas auditorias;
- × atualizações das avaliações de riscos e efetividade da gerência de risco e controles dos processos;
- × requisições dos acionistas e dos gestores da empresa;
- × grandes modificações na empresa, operações e controles;
- × oportunidades de melhorias;
- × mudanças no pessoal e nas especializações presentes na equipe.

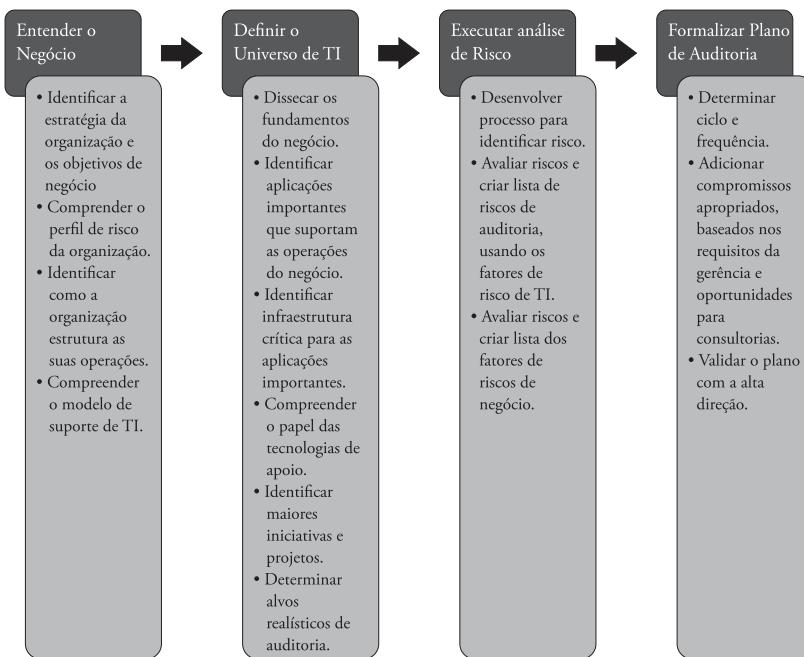
É importante que seja discutido como funcionará a integração da auditoria de sistemas de informação e a auditoria global, definindo qual a responsabilidade de cada equipe, pois, como discutido, a auditoria de sistemas de informação é influenciada pelos objetivos de negócio. Durante a auditoria dos sistemas, os auditores poderão ser confrontados com achados que fundamentam problemas não somente nos sistemas de informação, mas na estrutura de gerência e nos controles internos da empresa.

Na abordagem mais integrada de auditoria, a auditoria de sistemas de informação é parte integrante da auditoria global da empresa. Esta abordagem é um reflexo de como a Tecnologia de Informação tem se tornado um ativo estratégico para as organizações, portanto, cada vez mais, uma abordagem integrada é necessária.

O processo de planejamento da auditora interna, adotado pelo Instituto de Auditoria Interna, pode ser visualizado na figura 8.5, e é descrito no guia específico para desenvolver planejamento de auditorias de TI (REHAGE et al., 2008).

Este processo considera que, para a criação de um plano de auditoria interna, é necessário: a definição do universo auditado, e quais serão os sistemas de informação e serviços que irão estar englobados pela auditoria. Além disso, a construção de um bom plano de auditoria, deve considerar o gerenciamento de risco e as prioridades definidas da auditoria.

Figura 8.5 – Atividades de planejamento de auditoria



Fonte: Rehage et al (2008, p. 3).

Como é possível visualizar na figura 8.5, o primeiro passo será a compreensão do negócio auditado. Esta necessidade está alinhada com a auditoria moderna, em que um auditor não é só mais um verificador de números, mas sim um homem de negócio, pois busca preservar os melhores interesses do cliente da auditoria. Portanto, o planejamento da auditoria deve ser consistente com os planos de negócio da organização, considerando a estrutura atual da organização e o perfil de risco da empresa.

A equipe de auditoria deve estar ciente que a tecnologia existe para apoiar e alavancar os objetivos de negócio. Desta forma, antes de compreender o ambiente de TI, o auditor deve compreender a cultura, a visão, a missão e os valores da organização.

Os riscos devem ser observados considerando a *framework* de riscos utilizada na organização auditada. Caso não exista uma *framework* de risco na organização, será tarefa do auditor chefe escolher qual *framework* será utilizada. Durante o planejamento, devem ser considerados, além dos objetivos do sistema de informação, a aderência e a efetividade da governança, a gerência de riscos e controles internos.

Recursos para compreensão do negócio:

- × missão, visão e valores;
- × planos estratégicos;
- × planos anuais de negócio;
- × relatórios anuais aos acionistas;
- × formulários e questionários de órgãos reguladores.

Conhecer o negócio engloba a compreensão dos fatores ambientais de TI. Cada organização tem um ambiente de TI diferente, e este ambiente deve ser considerado durante a auditoria de sistemas de informação. As diferenças tecnológicas poderão requerer novos treinamentos ou alocação de auditores com conhecimento e experiências específicas.

Após a compreensão do negócio, passa-se a definir qual será o universo do negócio alvo da auditora. Para isso, será necessário apontar quais são os sistemas de informação mais significantes para a organização. Além dos sistemas de informação, é importante também identificar a infraestrutura que dá suporte a eles.

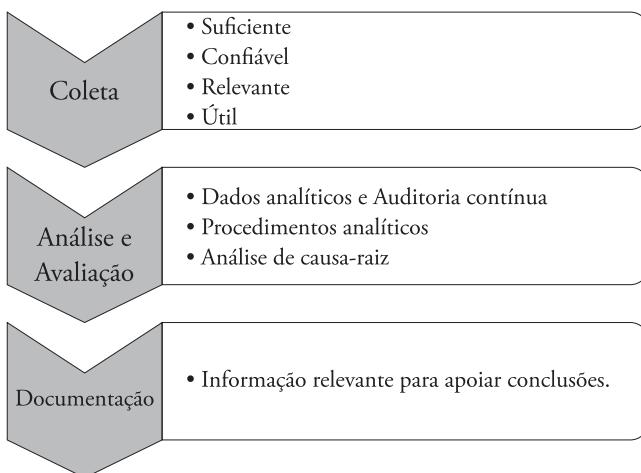
O planejamento deve utilizar técnicas de planejamento já utilizadas no mercado, tais como PMBOK e diagrama de GANTT. A auditoria é um projeto e deve ser bem planejada e executada.

× Execução

A fase de execução é centrada na coleta, análise e avaliação e documentação da informação relevante, este processo está ilustrado na figura 8.6.

Durante esta fase, será responsabilidade dos auditores internos identificar e coletar informações suficientes, confiáveis, relevantes e úteis para alcançar os objetivos da auditoria. A informação recolhida pelos auditores deve ser capaz de permitir que outras pessoas, após a análise dos dados, alcancem as mesmas conclusões do auditor. Por isso, é muito importante a identificação e recolhimento das informações para que os auditores não tenham conclusões com base em sentimentos, mas fundamentadas em análises e avaliações das evidências encontradas. Durante esta fase, o auditor executivo chefe deve verificar se os objetivos presentes no planejamento da auditoria estão sendo alcançados.

Figura 8.6 – Fase de execução da auditoria interna



Fonte: Elaborada pelo autor.

× Relatório

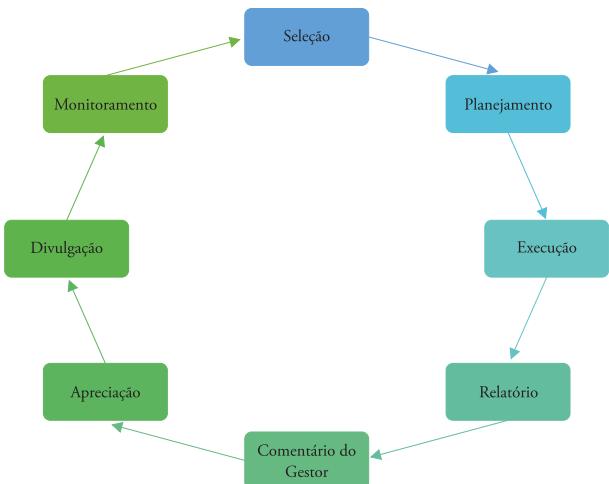
O objetivo desta fase é comunicar os resultados da auditoria. Os relatórios devem incluir o objetivo e escopo da auditoria, tais como, quando aplicáveis, as conclusões, recomendações e planos de ação, sempre de maneira precisa, objetiva clara, concisa, construtiva, completa e tempestiva. As técnicas para a construção de um bom relatório serão discutidas no próximo capítulo, e por este motivo não serão discutidas nesta seção.

8.2.2 Ciclo de Auditoria Operacional – TCU

O TCU propõe no Ciclo de Auditoria Operacional (ANOp) uma abordagem para avaliação com foco na gestão pública. A abordagem do TCU é fortemente influenciada pela INTOSAI, e pelas normas internacionais de entidades fiscalizadoras superiores (ISSAI).

Como definido pelo próprio manual ANOp, a auditoria operacional é o exame independente e objetivo da economicidade, eficiência, eficácia e efetividade de organizações, programas e atividades governamentais, com a finalidade de promover o aperfeiçoamento da gestão pública. O ciclo tem oito etapas: seleção, planejamento, execução, análise, elaboração de relatório, comentário do gestor, apreciação pela corte, divulgação e monitoramento. Por ser uma auditoria governamental, verificam-se algumas fases que não existem ou com grandes particularidades, quando comparadas a uma auditoria de

Figura 8.7 – Ciclo da auditoria operacional



Fonte: TCU (2010).

uma empresa privada, como: etapa de comentários do gestor, apreciação dos ministros do tribunal e divulgação pública do relatório. As etapas são apresentadas na figura 8.7:

8.2.2.1 Seleção

A etapa de seleção do objeto de auditoria visa selecionar um objeto que ofereça oportunidade para realização da auditoria, contribua para o aperfeiçoamento da administração pública e forneça à sociedade opinião independente sobre o desempenho da atividade pública. Esta seleção é importante para uma Entidade Fiscalizadora Superior (EFS), pois tem um amplo campo para auditar e recursos limitados. Deste modo, é necessário selecionar objetos de auditoria que contribuam para o aperfeiçoamento da gestão pública (TCU, 2010).

Além disso, são considerados critérios como: materialidade, relevância e vulnerabilidade.

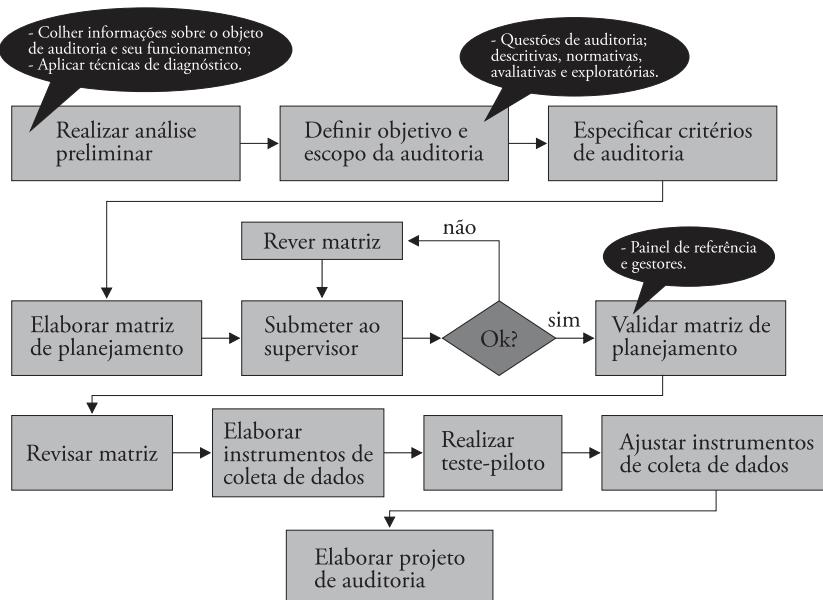
- ✖ **Materialidade:** considerar os valores auditados. Considerações em objetos de auditoria com alta materialidade têm grande possibilidade de gerar valor para a gestão pública. Deste modo, a materialidade de um sistema de informação que custou um alto valor é maior quando comparado a um software com baixo custo para a administração.
- ✖ **Relevância:** as auditorias devem ir ao encontro dos interesses da sociedade. Portanto, são considerados ao escolher objetos de auditoria a opinião dos parlamentares, técnicos das casas legislativas e figuras proeminentes da sociedade, relatos na imprensa, entre outros.
- ✖ **Vulnerabilidade:** situações em que são encontrados problemas de falta de informação, estruturas complexas ou planejamento inadequado, criam situações que possibilitam o surgimento de eventos adversos. Ao selecionar objetos de auditoria com estas características, aumenta-se a chance de poder contribuir com a gestão pública.

Esta etapa de seleção está aderente aos conceitos de auditoria moderna, portanto busca-se selecionar as áreas de maiores riscos, sejam eles materiais ou de imagem.

8.2.2.2 Planejamento

A fase de planejamento é responsável pela definição do projeto de auditoria, delimitando o objetivo, o escopo e a estratégia, além de estimar os recursos, os custos e o prazo necessários para a sua realização. A figura 8.8 detalha esta etapa.

Figura 8.8 – Atividades de planejamento



Fonte: TCU (2010).

São consideradas as seguintes atividades na etapa de planejamento:

- análise preliminar do objeto de auditoria;
- definição do objetivo e escopo da auditoria;
- especificação dos critérios de auditoria;
- elaboração da matriz de planejamento;
- validação da matriz de planejamento;
- elaboração de instrumentos de coleta de dados;

- g) teste-piloto;
- h) elaboração do projeto de auditoria.

A matriz de planejamento é um artefato que demonstra, para cada questão de auditoria, as informações necessárias para a análise; as fontes de obtenção das informações; os procedimentos de coleta e análise das informações; as limitações dela decorrentes; e os potenciais resultados esperados.

A matriz de planejamento e os instrumentos de coleta são testados com a execução do teste-piloto. Toda a equipe de auditoria deve estar envolvida nesta atividade. O teste deve ser executado em objetos de auditoria com dificuldade alta, permitindo que a equipe antecipe os problemas e valide o tamanho da amostra e a estratégia escolhida.

8.2.2.3 Execução

Nesta fase, a equipe de auditoria irá realizar os trabalhos de campo, incluindo as pesquisas necessárias à coleta de dados, por meio de entrevistas, aplicação de questionários, observação direta, grupos focais, consultas a documentos e bases de dados.

Saiba mais

Achado é a discrepância entre a situação existente e o critério, verificadas pelo auditor durante o trabalho de campo. O achado contém os seguintes atributos: critério (o que deveria ser), condição (o que é), causa (razão do desvio com relação ao critério) e efeito. Quando o critério é comparado com a condição existente, surge o achado de auditoria (ISSAI 3000/4.3, 2004 apud TCU, 2010).

Esta fase busca obter as evidências necessárias e suficientes para respaldar os achados e conclusões da auditoria. Os achados são discrepâncias entre a situação existente e o critério de avaliação, enquanto as evidências são as informações obtidas durante a auditoria, sejam evidências físicas, documentais, testemunhais ou analíticas, que fundamentam os achados. Após os trabalhos de campo, é criada a matriz de achados, cujo objetivo é sintetizar os resultados obtidos.

O resultado pode ser colocado em uma matriz de achado, que deve conter os seguintes campos:

- a) **achado** – fatos relevantes que foram encontrados pelo auditor durante a auditoria;
- b) **situação encontrada** – situação existente, identificada e documentada durante a fase de execução da auditoria;
- c) **critério** – legislação, norma, jurisprudência, entendimento doutrinário ou padrão adotado;
- d) **evidência** – informações obtidas durante a auditoria no intuito de documentar os achados e de respaldar as opiniões e conclusões da equipe;
- e) **causas** – o que motivou a ocorrência do achado;
- f) **efeitos** – consequências do achado.
- g) **encaminhamento** – propostas da equipe de auditoria. Deve conter identificação dos responsáveis.

8.2.2.4 Relatório

Um bom relatório deve registrar os achados de forma adequada. O conteúdo deve ser de fácil compreensão e não conter ideias vagas e ambíguas, e as informações contidas no relatório devem ser fundamentadas em evidências. Além disso, o relatório deve ser independente, relevante, objetivo, justo e construtivo.

O relatório é um dos principais resultados do trabalho de auditoria e, portanto, deve ser um trabalho de qualidade. Pode afetar a relevância e a credibilidade de toda a auditoria. Dada a importância de tal assunto, as técnicas para a criação de bons relatórios serão exploradas no próximo capítulo em seção específica para este assunto.

8.2.2.5 Comentários do gestor

Pelo caráter governamental dos relatórios do TCU, o auditado sempre deve ter oportunidade de examinar o relatório preliminar de auditoria antes que ele seja tornado público, entretanto, estes relatórios preliminares são sigilosos e não podem ser publicados pelos gestores.

Os gestores terão a possibilidade de apresentar novas informações que os auditores deverão avaliar e, se acharem relevantes, poderão esclarecer pontos do relatório ou até alterar o entendimento da equipe.

8.2.2.6 Apreciação

Nesta fase, os relatórios de auditoria são apreciados pelo Tribunal de Contas da União.

8.2.2.7 Divulgação

Esta etapa tem a finalidade de possibilitar à sociedade conhecer sobre os resultados das ações avaliadas. O controle social contribui para aumentar a efetividade do controle, por meio da mobilização da comunidade no acompanhamento e na apreciação dos objetivos, da implementação e dos resultados das políticas públicas.

8.2.2.8 Monitoramento

O monitoramento é uma fase de fiscalização, na qual o TCU verifica o cumprimento das deliberações e os resultados delas advindos, observando as providências adotadas e verificando os seus efeitos. O importante é que o monitoramento permite verificar, além da resposta das empresas às propostas da auditoria, a própria qualidade da auditoria, possibilitando identificar oportunidades de aperfeiçoamento, de aprendizado e de quantificação de benefícios.

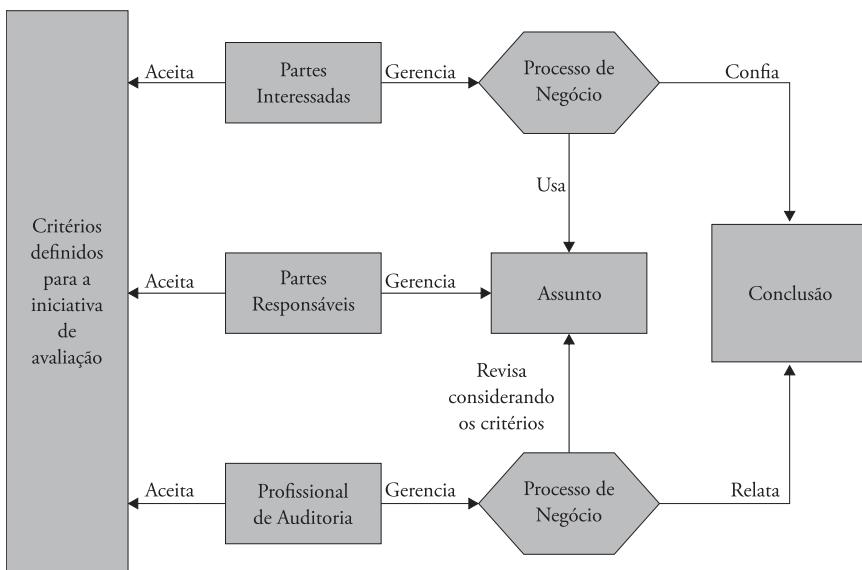
Esta etapa também subsidia o processo de seleção de novos objetos de auditoria. As informações apuradas nos monitoramentos são usadas para calcular o percentual de implementação de deliberações e a relação custo/benefício das auditorias, indicadores de efetividade da atuação das entidades de fiscalização superior.

8.2.3 ISACA

A ISACA disponibiliza alguns guias importantes, entre eles o *IT Assurance Guide*. O título pode ser traduzido como Guia de Avaliação de TI, e foca na avaliação dos controles internos de TI descritos no COBIT. No título, é usado o termo *Assurance*, ou avaliação. Este termo é mais abrangente do que o termo auditoria, no entanto a auditoria é um tipo de avaliação.

Para manter a coesão do capítulo, substituiremos o termo *assurance* para auditoria nesta seção. Esta abordagem é muito focada na avaliação dos controles internos da organização, como está desenhado na figura 8.9. O objetivo é verificar se os critérios definidos para a auditoria são atendidos pelos processos de negócio e também pelas partes responsáveis por gerenciar a organização. Nesta abordagem, usualmente inconformidades estão relacionadas a problemas com os controles dos processos e as recomendações geradas da auditoria também terão este foco.

Figura 8.9 – Relacionamento entre os componentes de uma iniciativa de avaliação



Fonte: ISACA (2007).

Este guia foi criado com o intuito de avaliar a implantação dos controles de objetivos propostos pelo COBIT (ISACA, 2007) , apesar de ter sido criado de modo genérico e, portanto, poder ser utilizado para outros fins além da implantação do COBIT. Ele está organizado em três etapas (figura 8.10): planejamento, escopo e execução. Estas apresentam grande relacionamento com as atividades apresentadas nas outras abordagens.

Figura 8.10 – Etapas do processo de implantação do COBIT



Fonte: ISACA (2007).

8.2.3.1 Planejamento

O primeiro passo para a fase de planejamento é o estabelecimento do universo de avaliação. Para a criação do plano, é necessário que o profissional de auditoria combine a compreensão de tecnologia da informação e a seleção de uma *framework* de controle interno, no caso o COBIT. A escolha da *framework* funciona como a definição dos critérios na abordagem da IPPF.

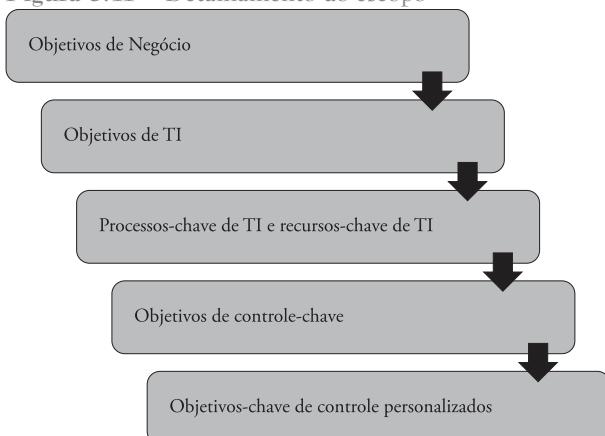
Na abordagem da ISACA, o planejamento somente é criado após a execução de uma avaliação de alto nível do estado atual da organização, com o objetivo de detectar riscos e pontos de atenção. No final desta fase, deverá existir um plano de auditoria de TI.

8.2.3.2 Escopo

A fase do escopo é o momento em que será selecionado o universo a ser avaliado, definindo o escopo e o objetivo da auditoria de TI. O quanto detalhada será a definição do escopo irá depender da complexidade da auditoria a ser realizada.

A definição do escopo e o detalhamento são cruciais para uma boa

Figura 8.11 – Detalhamento do escopo



Fonte: Elaborada pelo autor.

avaliação. Caso seja feita uma avaliação muito superficial, as conclusões não serão verdadeiras. Caso seja muito detalhista, poderá afetar os prazos e custos da avaliação. A figura 8.11 apresenta o detalhamento do escopo.

8.2.3.3 Execução

A terceira etapa é a execução do plano de auditoria de TI, por meio dele será gerado o resultado final da auditoria. A auditoria ocorre por meio de avaliações do projeto dos controles da organização, da confirmação da operação dos controles e de qual a efetividade operacional dos controles. Para verificar a efetividade do controle, é necessário avaliar evidências diretas e indiretas do impacto dos controles na qualidade do processo, como por exemplo avaliar as características do processo antes da implantação do controle e após a implantação do controle, e depois verificar como o controle afetou o processo. Os achados serão relatados em um relatório final com as conclusões e recomendações do auditor.

8.3 Auditoria e padrões ISO

Existem padrões ISO para muitas das necessidades existentes em uma empresa. Também existe um processo para tratar auditoria de sistemas. A ISO 19011:2012 (ABNT, 2012) apresenta um guia para auditoria de sistemas de gestão, entretanto no próprio padrão é relatada a possibilidade da aplicação da norma para outros tipos de auditoria de sistemas de informação.

Saiba mais

A Norma ISO 19011:2012 não estabelece requisitos, mas fornece diretrizes sobre a gestão de um programa de auditoria, sobre o planejamento e a realização de uma auditoria de sistema de gestão, bem como sobre a competência e avaliação de um auditor e de uma equipe auditora.

Uma das diferenças do método proposto pela ISO 19011 em relação a outros apresentados até o momento é que ele possui foco exclusivo na auditoria de sistemas, e não nas relações da auditoria com a necessidade dos acionistas ou

da organização. Por isso, é uma abordagem interessante, quando a necessidade da auditoria da informação está menos relacionada a uma necessidade da alta gerência e sim por requisitos objetivos de sistemas de informação.

Outro padrão ligado à auditoria é a ISO 17021:2006, um padrão para avaliação de conformidade e requisitos para organizações que fornecem auditoria e certificações para sistemas de gestão. Enquanto a norma 19011 trata das diretrizes para realização de auditorias, a ISO 17021 trata dos requisitos que as empresas que realizaram auditoria deverão atender. Portanto, é um padrão para empresas que realizam auditorias externas ou, como chamadas pela ISO, auditoria de terceira-partes.

A ISO 19011 utiliza uma abordagem em cinco etapas até a sua conclusão, como demonstrado na figura 8.12. As etapas são: iniciando a auditoria; realizando a análise crítica de documentos; preparando as atividades da auditoria; conduzindo as atividades da auditoria; preparando, e aprovando e distribuindo o relatório de auditoria.

Figura 8.12 – Visão geral das atividades típicas de auditoria



Fonte: Elaborada pelo autor.

8.3.1 Iniciando a auditoria

Na ISO 19011 não existe o papel do auditor chefe executivo. Um auditor líder é escolhido no inicio da auditoria, que observa Apenas observa o conflito de competências caso haja outras auditorias acontecendo conjuntamente na empresa.

Nesta fase também são definidos os objetivos, o escopo e os critérios da auditoria. Alguns objetivos já sugeridos pela ISO são:

- a) determinação da extensão da conformidade do sistema de gestão do auditado, ou partes dele, com o critério de auditoria;
- b) avaliação da capacidade do sistema de gestão para assegurar a concordância com requisitos estatutários, regulamentares e contratuais;
- c) avaliação da eficácia do sistema de gestão em atingir seus objetivos especificados;
- d) identificação de áreas do sistema de gestão para potencial melhoria.

Nesta abordagem, os objetivos da auditoria são definidos pelo cliente da auditoria e o escopo e critérios da auditoria são definidos em acordo entre líder da auditoria e cliente. Esta é uma diferença a ser considerada.

8.3.2 Realizando a análise crítica de documentos

Esta fase tem como objetivo avaliar se, de acordo com a documentação existente, o sistema está aderente ao estatuto, lei ou requisito definido. Deverá ser averiguado se a informação contida na documentação está completa, correta, consistente e atual.

Caso a documentação seja considerada inadequada, a auditoria poderá ser suspensa até a resolução deste fato.

8.3.3 Preparando as atividades de auditoria

Esta é a fase da construção do plano de auditoria. O plano deverá proporcionalmente criterioso em detalhes ao tamanho do escopo e à complexidade da auditoria.

De acordo com a ISO (2012, p. 20), convém que o plano de auditoria inclua o seguinte:

- a) os objetivos da auditoria;
- b) o critério de auditoria e qualquer documento de referência;
- c) o escopo da auditoria, inclusive com identificação das unidades organizacionais e funcionais e processos a serem auditados;
- d) as datas e lugares onde as atividades de auditoria no local serão realizadas;
- e) o tempo esperado e a duração de atividades de auditoria no local, inclusive reuniões com a direção do auditado e reuniões da equipe da auditoria;
- f) as funções e responsabilidades dos membros da equipe da auditoria e das pessoas acompanhantes;
- g) a alocação de recursos apropriados para áreas críticas da auditoria.

Convém que o plano de auditoria também inclua o seguinte, se apropriado:

- a) identificação do representante do auditado na auditoria;
- b) o idioma de trabalho e do relatório da auditoria, se ele for diferente do idioma do auditor e/ou do auditado;
- c) os principais pontos do relatório de auditoria;
- d) arranjos de logística (viagem, instalações no local etc.);
- e) assuntos relacionados a confidencialidade;
- f) quaisquer ações de acompanhamento de auditoria.

O planejamento deverá designar responsabilidades a cada membro da equipe para auditar processos específicos, funções, locais, áreas ou atividades. Esta designação deverá considerar a competência e uso eficaz dos recursos e também a independência dos auditores. O líder da auditoria deve verificar se existe algum fato que poderá influenciar a independência de um auditor na designação de uma atividade de auditoria.

No fim desta fase, a equipe de auditoria também deverá ter posse das listas de verificações, de acordo com os critérios pré-estabelecidos e planos de amostragem dos ativos a serem auditados.

8.3.4 Conduzindo atividades de auditoria

Esta é a fase em que acontecerá a coleta de informações para gerar as evidências da auditoria. As fontes de informação da auditoria podem ser:

- a) entrevista com os empregados e outras pessoas;
- b) observações de atividades e do ambiente e condições de trabalho circunvizinho;
- c) documentos, como política, objetivos, planos, procedimentos, normas, instruções, licenças e permissões, especificações, desenhos, contratos e ordens;
- d) registros, como registros de inspeção, notas de reuniões, relatórios de auditoria, registros de monitoramento de programas e resultados de medições;
- e) resumos de dados, análises e indicadores de desempenho;
- f) informações sobre os programas de amostragem do auditado e sobre procedimentos para o controle de amostragem e processos de medição;
- g) relatórios de outras fontes, como por exemplo, realimentação de cliente, outras informações pertinentes de partes externas e classificações de fornecedor;
- h) bancos de dados computadorizados e web sites.

As evidências de auditoria encontradas serão avaliadas conforme os critérios de auditoria especificados durante as fases iniciais, esta análise dará suporte às constatações da auditoria. E, por fim, a análise destas constatações irá fundamentar a conclusão da auditoria. A conclusão da auditoria inclui a análise crítica das constatações da auditoria a preparação de recomendações, caso seja especificado nos objetivos da auditoria, e uma discussão sobre os planos de acompanhamento da auditoria.

8.3.5 Preparando, aprovando e distribuindo o relatório de auditoria

A confecção do relatório da auditoria é responsabilidade do líder da equipe. É importante que o relatório contenha todos os registros da auditoria, de modo claro, conciso e preciso. O resultado da auditoria é de propriedade do cliente da auditoria, salvo legislação em contrário.

Após a conclusão da auditoria, em alguns casos, a equipe de auditoria poderá acompanhar algumas ações corretivas, preventivas ou de melhoria sugeridas durante o programa de auditoria. Estas ações não fazem mais parte da auditoria e devem ser tomados os cuidados para evitar que de alguma maneira seja afetada a independência da equipe de auditoria nos próximos compromissos de auditoria.

8.4 ISO série 27000

Na série ISO 27000 a auditoria de sistemas desempenha um papel muito relevante, dando credibilidade às instituições sobre as medidas de segurança de informação implantada. A auditoria destas medidas é importante principalmente no mercado bancário. A ISO 27000 utiliza uma abordagem baseada no ciclo *plan, do, check, act*. Um dos modos possíveis de executar a fase de verificação (*check*) é uma auditoria de Sistemas de Informação.

Como esperado, auditorias da ISO 27000 são fortemente focadas na segurança dos sistemas de informação, e isto irá influenciar fortemente na capacidade técnica e conhecimento requerido dos profissionais de auditoria. Além disso, a ética deverá ter um peso muito maior para contratação dos profissionais que atuarão com Segurança da Informação.

Síntese

O estudo dos métodos de auditoria de informação é muito importante para um auditor de sistemas de informação. Como foi discutido neste capítulo, muito da metodologia de auditoria de sistemas de informação é aproveitada do conhecimento adquirido durante anos de auditorias contábeis e de outras áreas. Desprezar este conhecimento seria retrabalho.

No entanto, é importante reconhecer as diferenças e particularidades das áreas de tecnologia, principalmente dos sistemas de informação. Estas diferenças deverão sempre ser consideradas no planejamento de uma auditoria de sistemas de informação.

É importante que o auditor utilize o método adequado para executar a auditoria de sistemas de informação para evitar ataques a credibilidade da auditoria. Uma auditoria poderá dar suporte para alterações no funcionamento de uma empresa, demissões, contratações e até fundamento a processos jurídicos. A utilização de métodos reconhecidos dará credibilidade a sua auditoria.

Atividades

1. Discuta o papel do auditor chefe executivo para a auditoria interna, segundo a IIA.
2. (CESPE-UNB) A respeito de auditoria interna, assinale a opção correta de acordo com o IIA (Institute of Internal Auditors).
 - a) As normas de atributos se restringem às características dos profissionais que realizam as atividades de auditoria.
 - b) As regras de conduta do auditor interno limitam-se a três aspectos: discrição, integridade e objetividade.
 - c) A auditoria interna é uma atividade de avaliação e consultoria, independente e objetiva, desenvolvida para agregar valor e melhorar as operações da organização.
 - d) Os serviços de avaliação normalmente compreendem dois participantes: o auditor interno e o cliente do trabalho.
 - e) Normas de atributos, de desempenho e de responsabilização correspondem aos tipos de normas a serem seguidas pela auditoria.
3. Qual a importância da metodologia para a Auditoria de Sistemas de Informação?
4. Quais as principais diferenças entre auditorias externas e internas?

9

Técnicas e Melhores Práticas de Auditoria de Sistemas de Informação

ABORDAREMOS NESTE CAPÍTULO algumas técnicas e melhores práticas de auditoria de sistemas de informação, de forma que os administradores de sistemas tenham conhecimento aprofundado sobre o processo de auditoria de SI.

TAMBÉM DETALHAREMOS o processo de construção de um relatório de auditoria de SI, desde a sua preparação, passando pela escrita e até sua finalização, detalhando todas as etapas necessárias para que um trabalho de auditoria seja bem conduzido.

Objetivo de aprendizagem:

- × Aplicação prática para auditoria de sistemas de informação.

9.1 Técnicas de auditoria de sistemas de informação

Quando um administrador de sistemas ouve a palavra “auditoria”, logo lhe vem à mente a imagem de alguma inspeção surpresa que tentará expor as fraquezas dos sistemas de informação. Todavia, como responsável pela segurança da informação, ele não só deve querer, como insistir em auditorias anuais completas em seus sistemas.

Uma auditoria pode variar bastante o seu escopo, começando desde a análise de um arquivo de log (do tipo *sysadmin*) até uma análise em grande escala de práticas de negócios. O escopo de uma auditoria dependerá das metas as quais se deseja alcançar.

O ideal é que o administrador não espere que ocorra um ataque bem-sucedido em sua organização, de forma que o obrigue a contratar um auditor. As auditorias anuais estabelecem uma linha de base de segurança com as quais os gestores podem medir o progresso e avaliar o conselho profissional do auditor. Uma postura de segurança estabelecida também ajudará a medir a eficácia da equipe de auditoria. Mesmo se a empresa usar auditores diferentes a cada ano, o nível de risco descoberto deve ser consistente ou até mesmo diminuir ao longo do tempo. A menos que tenha havido uma revisão dramática da infraestrutura da organização, o aparecimento súbito de exposições críticas de segurança após anos de bons relatórios lança uma profunda sombra de dúvida sobre as auditorias anteriores.

Se a empresa não tiver anos de análises de segurança internas e externas para servir de linha de base, deve considerar a utilização de dois ou mais auditores trabalhando separadamente para confirmar as descobertas. Pode ser dispendioso, mas não tanto como seguir conselhos ruins. Se não for prático envolver equipes de auditoria paralelas, ao menos deve-se procurar uma segunda opinião sobre os resultados da auditoria que exigiram um trabalho extenso.

Existem variadas metodologias de auditoria utilizadas no mercado que podem ser chamadas de técnicas. Elencaremos a seguir algumas destas técnicas, apresentadas por Lyra, 2008.

9.1.1 Técnica de inserção de dados de teste

Esta técnica também é conhecida como “*test data*” ou “*test deck*”, e envolve o uso de um conjunto de dados especialmente projetados e preparados com o objetivo de testar as funcionalidades de entrada de dados no sistema.

Também verifica a existência e a eficácia de controles programados nos sistemas. Antes das transações serem executadas, os resultados de teste esperado são predeterminados (calculados com base no pressuposto de que o sistema que está sendo testado contém controles internos efetivos e funcionará conforme especificado), para que os resultados reais possam ser comparados com os resultados predeterminados.

Os tipos gerais de condições que devem ser testadas incluem, mas não se limitam a:

- ✖ **testes de transações que ocorrem normalmente** – para testar a capacidade de um sistema processar com precisão dados válidos, os testes devem incluir transações que ocorrem durante a utilização normal do sistema. Por exemplo, em um sistema de folha de pagamento as transações que ocorrem normalmente incluem o cálculo do salário regular, pagamento de horas extras e algum outro tipo de pagamento adicional;
- ✖ **testes usando dados inválidos** – testar a existência ou a eficácia dos controles programados de modo que dados inválidos sejam rejeitados ou registrados em log de erros. Como exemplo, podemos citar:
 - a) caracteres alfabéticos quando caracteres numéricos são esperados e vice-versa;
 - b) dados incompletos ou irregulares em campos de dados específicos;
 - c) entrada de dados em condições que violem limites estabelecidos por lei ou por procedimentos operacionais padrão.

Esta técnica também pressupõe que os dados sejam abrangentes e verifiquem principalmente os limites de cada intervalo permitido para as variáveis. Quanto mais combinações de transações puderem ser feitas no arquivo de carga, maior será a cobertura do teste.

- ✗ **Vantagens:** não é necessário um avançado conhecimento de informática para a elaboração dos dados, o qual pode ser feito inclusive utilizando-se de softwares automatizados que tornam a tarefa mais simples.
- ✗ **Desvantagens:** existe uma dificuldade inerente em antecipar e planejar todas as combinações possíveis de entrada de dados que podem existir no ambiente de uma organização.

9.1.2 Técnica de facilidade de teste integrado

A técnica de facilidade de teste integrado (ITF – *Integrated Test Facility*) é uma técnica na qual dados de teste são introduzidos nos ambientes reais de processamento utilizando-se versões correntes da produção. Os auditores criam uma espécie de empresa fictícia nos arquivos processados pelo sistema de aplicação. Por exemplo, em um sistema de folha de pagamento, os auditores podem criar registros para um funcionário fictício ou clientes inexistentes nas contas a receber. Os auditores então submetem os dados do teste ao sistema de aplicativos como parte da transação normal de dados inseridos no sistema. Eles monitoram os efeitos de seus dados de teste na entidade fictícia que foi criada anteriormente.

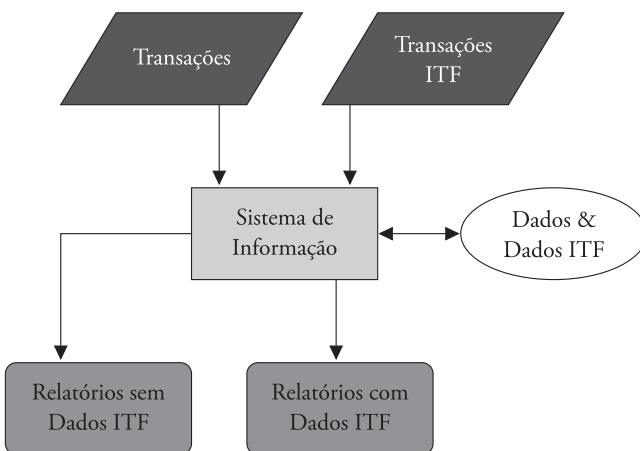
Duas grandes decisões devem ser tomadas quando os auditores usam a ITF. Primeiro, os auditores devem determinar qual método será usado para a inserção de dados de teste. Uma abordagem é selecionar e marcar transações em tempo real. As transações marcadas então atualizam não apenas seus registros de destino, mas também a entidade fictícia que foi previamente criada. Uma abordagem alternativa para esta primeira decisão é projetar e criar operações de teste específicas para a aplicação. Essas transações de teste atualizam apenas a entidade fictícia.

A segunda decisão é que os auditores devem determinar como os efeitos das transações de teste serão marcados dentro do sistema de aplicação que

está sendo testado. Uma primeira abordagem é submeter as transações que têm valores imateriais e que, portanto, não são susceptíveis à observação pelos usuários do sistema de aplicativos. Uma segunda abordagem é modificar o sistema de aplicativos para que as transações de teste não sejam contadas nos totais de controle do sistema de aplicativos. Esta segunda abordagem é a mais cara, mas muitas vezes é a mais eficaz.

A figura a seguir exemplifica esta técnica de forma resumida.

Figura 9.1 – Técnica ITF de auditoria de sistemas



Fonte: Elaborada pelo autor.

- ✖ **Vantagens:** por funcionar no ambiente de produção da empresa, a técnica não acarreta custo adicional ou ambiente de processamento exclusivo.
- ✖ **Desvantagens:** devido ao fato de que dados de testes são misturados com dados reais, isto acarreta um trabalho adicional e operacional para a realização do estorno destas transações, causando efeitos que demandam atenção redobrada. A quantidade de dados fictícios precisa ser limitada, de modo que não venha a comprometer o desempenho do sistema em produção. Também existe a possibilidade de contaminação da base real com dados fictícios, causando grandes transtornos para a organização.

9.1.3 Técnica de simulação paralela

A simulação paralela processa os dados reais do cliente por meio de um programa de auditoria especialmente desenvolvido e que atende a toda a lógica necessária para o teste, simulando as funcionalidades do programa em produção. De forma frequente, embora não necessariamente, o processamento é realizado no computador do auditor. Após o processamento dos dados, o auditor compara a saída obtida do seu programa com a saída obtida do cliente. O método, então, verifica o processamento de transações reais (em contrapartida a outras técnicas, como a de dados de teste e ITF que usam transações simbólicas) e permite que o auditor verifique os resultados reais do cliente. Esse método permite que um auditor simplesmente teste porções do sistema para reduzir o tempo total e se concentrar em controles-chave.

- × **Vantagens:** não existe custo de preparação de massas de dados fictícios como em outras técnicas. Pode-se também processar um grande volume de dados, eliminando dúvidas que amostras pequenas e não-abrangentes podem apresentar.
- × As **desvantagens** deste método incluem:
 - × o tempo que leva para construir uma duplicata exata do sistema do cliente;
 - × incompatibilidade entre o software do auditor e o software do cliente;
 - × o rastreamento das diferenças entre os dois conjuntos de resultados com as diferenças nos programas pode ser difícil;

o tempo envolvido no processamento de grandes quantidades de dados.

9.1.4 Lógica de auditoria embutida nos sistemas

Esta técnica consiste em incluir a lógica de auditoria nos sistemas na fase de desenvolvimento. Uma das maneiras de implementar é efetuar a impressão periódica dos relatórios de auditoria e logs do sistema para revisão e acompanhamento dos procedimentos operacionais.

- × **Vantagens:** as atividades do sistema podem ser monitoradas permanentemente por meio de acesso do auditor. Esta técnica tam-

bém não apresenta restrição quanto à entrada de dados que podem ser incluídos.

- ✖ **Desvantagens:** por exigir um custo adicional de desenvolvimento, pode aumentar custos e acarretar também perda de desempenho devido à alocação de recursos.

9.2 Melhores práticas de auditoria de sistemas de informação

Existem algumas orientações sobre os tipos específicos de habilidades e técnicas de auditoria que se referem à melhoria das habilidades de comunicação, preparação de relatórios de auditoria e planos de ação e implementação de métodos para seleção de amostras na auditoria. Em alguns casos, pode ser necessário adaptar os procedimentos para refletir a situação em uma determinada organização.

A falta de padrões para a auditoria de sistemas dificulta muito a vida dos profissionais desta área. Embora não esteja convencionado um padrão único aceito pelo mercado, procuramos apresentar as melhores práticas recomendadas pelas associações reconhecidas mundialmente como detentoras de amplo conhecimento no assunto.

9.2.1 Reuniões de abertura com a alta administração

A reunião de abertura com a alta administração é muito importante. Ela define o tom para toda a auditoria e fornece a oportunidade de estabelecer o ambiente adequado para começar a construir relações de trabalho eficazes. Na reunião de abertura os auditores devem explicar o papel da auditoria e enfatizar que o objetivo principal é fornecer ajuda construtiva e aconselhamento à gestão, bem como discutir e acordar o escopo e os objetivos da auditoria.

Também deve ser discutido o calendário da auditoria e quaisquer dificuldades que possam surgir, por exemplo, ausência de pessoal-chave, desenvolvimento de novos sistemas etc. Deve-se estabelecer os procedimentos que serão adotados para a confirmação dos resultados da auditoria, além de discutir o projeto de relatório. Devem ser também estabelecidas as horas normais de trabalho, especialmente se algum trabalho for feito fora dos escritórios da

organização e qualquer outra rotina do escritório, a fim de facilitar a organização de reuniões, localizar pessoas etc.

O auditor deve deixar claro que precisará acessar todos os arquivos e documentos relevantes, bem como solicitar o uso de um escritório compatível com suas atividades durante o curso da auditoria, se necessário.

9.2.2 Entrevistas

As entrevistas são uma parte fundamental do processo de auditoria. Elas são uma forma importante de obter e confirmar informações e fatos sobre como os sistemas e controles estão sendo operados. Ao mesmo tempo, representam uma oportunidade para criar e manter boas relações entre departamento/empresa de auditoria e seus clientes.

Existem dois tipos de entrevista: diretivas e não-diretivas. As entrevistas diretivas destinam-se a obter informações específicas sobre fatos verificáveis, por exemplo, o procedimento para o pagamento de faturas de compra. Neste tipo de reunião o auditor planeja a reunião para estabelecer que informação é necessária e determina perguntas que fornecerão essa informação. O auditor controla toda a reunião, definindo o tom e o ritmo e mantendo a discussão em linha com os objetivos planejados.

Em contrapartida, a entrevista não-diretiva tem como objetivo obter compreensão e construir uma relação de confiança com o auditado. As perguntas diretas são evitadas e a entrevista é estruturada apenas na medida em que o auditor identifica e abre grandes áreas de discussão. Esta abordagem tem potencial para descobrir novas áreas para auditoria, mas elas têm de ser bem controladas ou poderão tornar-se muito longas e demoradas.

Não há o “melhor” método de entrevistas. A abordagem depende da pessoa entrevistada, da natureza da auditoria, do tipo de informação necessária e do tempo disponível. Em muitos casos, as entrevistas são uma combinação das duas abordagens, começando com uma abordagem diretiva para obter as informações necessárias e terminando com uma abordagem não-diretiva para permitir que o entrevistado amplie a discussão.

9.2.3 Comitê de padrões da associação de controle e auditoria de tecnologia da informação

Existe uma série de recomendações emitidas pelo Comitê de Padrões da Associação de Controle e Auditoria de TI dos EUA, acerca dos trabalhos do auditor de sistemas de informação. Lyra (2008) elenca estas recomendações, as quais apresentamos resumidas a seguir:

- ✖ **responsabilidade, autoridade e prestação de contas** – a responsabilidade, autoridade e prestação de contas sobre a função do auditor de sistemas de informação devem ser documentadas de forma apropriada em uma carta proposta ou de aderência ao escopo;
- ✖ **independência profissional** – a independência deve ser em todas as questões relacionadas à tecnologia da informação, especialmente no relacionamento organizacional;
- ✖ **ética profissional e padrões** – o auditor deve atentar para o cumprimento do zelo profissional, em todos os aspectos de seu trabalho;
- ✖ **competência** – é necessário que o auditor possua competência técnica suficiente para a execução de seu trabalho. Deverá também manter esta competência técnica por meio de aprimoramento constante, visto que as inovações tecnológicas se modificam constantemente;
- ✖ **planejamento** – o planejamento é fundamental para direcionar os objetivos da auditoria e seguir os padrões profissionais aplicáveis. Ao final da tarefa deverá obter evidências suficientes, confiáveis, relevantes e proveitosas para alcançar efetivamente os objetivos da auditoria;
- ✖ **emissão de relatório** – a emissão de relatório será detalhada de forma mais ampla no tópico 9.3;
- ✖ **atividades de follow-up** – o auditor deve requisitar informações sobre recomendações e conclusões anteriores para determinar se ações apropriadas foram implementadas em tempo hábil.

9.3 Relatório de auditoria de sistemas de informação

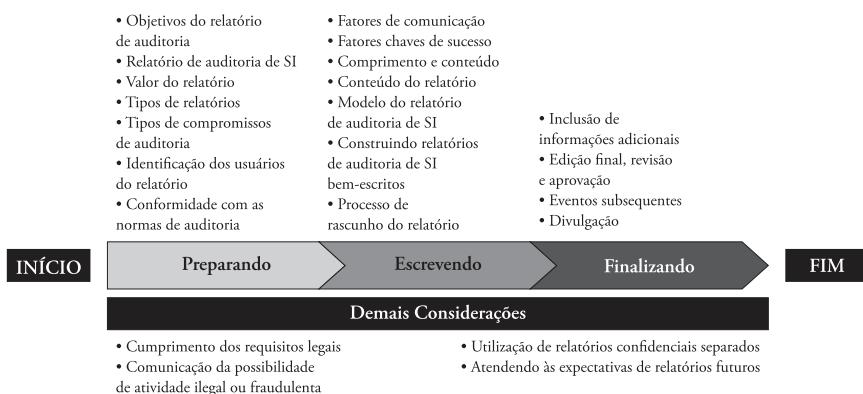
Faremos a seguir a apresentação de uma metodologia para desenvolvimento de um relatório de auditoria de sistemas de informação. O objetivo é auxiliar na elaboração de um relatório de auditoria comprehensível e bem apoiado que cumpra os requisitos das Normas de Auditoria e Garantia dos Sistemas de Informação e das Diretrizes de Auditoria e Garantia de SI que são publicadas pela ISACA. A orientação também é projetada para ajudar a garantir que o resumo do trabalho de auditoria e os resultados da auditoria sejam claramente apresentados e que o relatório de auditoria do SI apresente os resultados do trabalho realizado de forma clara, concisa e completa.

Esta orientação é aplicável às auditorias de SI que são realizadas por auditores internos, externos ou governamentais, embora a ênfase que é colocada no conteúdo do relatório pode variar dependendo do tipo de envolvimento da auditoria e por quem ela é realizada.

9.3.1 Processo de escrita de um relatório de auditoria de SI

O processo de redação de um relatório de auditoria de SI inclui três fases, como mostrado na figura 9.2 a seguir.

Figura 9.2 – Fases da escrita do relatório de auditoria de SI



Fonte: ISACA (2015).

Cada fase inclui etapas fundamentais para ajudar a garantir que o relatório final de auditoria de SI seja compreensível, atenda às necessidades de seus leitores e esteja em conformidade com os padrões de auditoria. Para ser compreensível, o relatório deve ser bem escrito e bem organizado. Também é preciso tomar decisões sobre a linguagem, a legibilidade e o nível de explicação necessário para ajudar o público-alvo a compreender os termos técnicos, a complexidade dos sistemas de TI e os processos de negócio.

Para atender às necessidades dos leitores, o auditor precisa identificar o público primeiro e, em seguida, determinar como vários grupos de leitores utilizam o relatório de auditoria. Dependendo da distribuição do relatório, o público pode ter vários graus de conhecimento técnico. Tornar os resultados da auditoria compreensíveis para cada grupo afeta o conteúdo e a apresentação do relatório. Além disso, a devida diligência deve ser exercida durante todo o processo de redação do relatório para garantir a exatidão, integridade e validade do conteúdo do relatório, além da conformidade com as normas e diretrizes de auditoria e garantia ISACA, e quaisquer outros requisitos obrigatórios. Além do que, deve ter aderência aos protocolos de comunicação que são estabelecidos pelas organizações de auditoria. A seguir faremos uma explanação resumida de cada uma das três fases, e na sequência um detalhamento maior de cada uma delas:

- ✖ **fase 1 – preparando a escrita:** na primeira fase o foco é sobre os requisitos de conteúdo, complexidade do assunto, normas de auditoria e orientações gerais. A primeira fase também inclui a determinação da estrutura do relatório e, dependendo da duração esperada dos trabalhos, um resumo executivo, um sumário ou apêndices podem ser necessários. Se a equipe de auditoria já tiver estabelecido a estrutura do relatório, um esboço ou modelo poderá ajudar o auditor com o processo de escrita. Durante a primeira fase, certos detalhes como entidades, títulos, número de compromissos e período de auditoria podem ser inseridos no modelo de relatório.
- ✖ **fase 2 – escrevendo o relatório:** durante a fase de elaboração do relatório os detalhes específicos sobre o escopo da auditoria, objetivos, metodologia, conclusões e recomendações são extraídos dos documentos de trabalho e inseridos no modelo de relatório. Uma introdução do relatório e um sumário executivo podem necessitar ser escritos nesta fase. E os resultados da auditoria precisam ser redigidos

de forma a incluir as conclusões e achados. O resultado desta fase é um projeto de relatório formal que pode ser apresentado ao auditado para a sua revisão, *feedback* e fornecimento de uma resposta da gestão ou respostas às conclusões do relatório e recomendações.

- × **fase 3 – finalização do relatório:** a fase de finalização do relatório prepara o relatório final de auditoria para emissão ao auditado e quaisquer outras partes designadas. Questões de gestão de auditoria são inseridas no relatório com possíveis respostas do auditor, e as decisões finais são feitas a respeito do conteúdo do relatório, relatando eventos subsequentes ou divulgações, distribuição e conformidade com as normas de auditoria e outros requisitos.

9.3.2 Fase 1 – preparando a escrita

A fase 1 (preparação da escrita) consiste em elencar os objetivos principais, relatório de auditoria, valor do relatório, tipos de relatório, tipos de compromissos de auditoria, descrição dos compromissos, identificação dos usuários do relatório e conformidade com as normas de auditoria. Explicaremos de forma mais detalhada nos tópicos subsequentes.

9.3.2.1 Objetivos dos relatórios de auditoria

Os seis objetivos principais do relatório de auditoria são:

- × apresentar formalmente os resultados da auditoria ao auditado (e ao cliente de auditoria se diferente do auditado);
- × servir como encerramento formal do trabalho de auditoria;
- × fornecer declarações de segurança e, se necessário, identificação de áreas que requerem ações corretivas e recomendações relacionadas;
- × servir como uma referência valiosa para qualquer parte que pesquise a entidade ou tópico de auditoria;
- × servir como base para uma auditoria de acompanhamento se os resultados da auditoria forem apresentados;
- × promover a credibilidade da auditoria quando bem desenvolvida e bem escrita.

Os objetivos de relatórios específicos de auditoria de SI são desenvolvidos com base nos requisitos dos gestores e de outros usuários do relatório, em conformidade com os padrões de auditoria de SI e os protocolos de organização de auditoria. O cliente ou outras partes interessadas, tais como organizações de supervisão, são identificados durante o planejamento da auditoria. O auditor desenvolve o escopo e os objetivos da auditoria considerando esses requisitos e outros elementos do planejamento, tais como avaliações de risco, materialidade e adequação dos controles declarados, juntamente com requisitos de governança reguladora e de TI. O relatório de auditoria apresenta formalmente a finalidade e os resultados de acordo com estes requisitos.

Todo relatório de auditoria deve fornecer respostas imparciais e bem apoiadas aos objetivos iniciais. Por exemplo, se o objetivo for determinar se os controles adequados estão em vigor para fornecer uma garantia razoável de que somente pessoas autorizadas podem acessar o *datacenter*, o relatório deve indicar a conclusão ou opinião do auditor sobre a adequação dos controles para atingir este objetivo. Se os controles tiverem de ser implementados ou reforçados para atingir o objetivo, o relatório deve fornecer uma recomendação para satisfazer essa necessidade.

9.3.2.2 Relatório de auditoria de SI

O relatório é o principal meio de comunicar os resultados de uma auditoria ao cliente ou entidade auditada, órgãos de supervisão ou outras partes interessadas. Os relatórios também são distribuídos a partes externas, como o público em geral ou agências governamentais que têm autoridade reguladora sobre a entidade de auditoria. Embora existam várias maneiras pelas quais os auditores podem manter um nível profissional de transparência e manter a administração informada sobre o escopo, os objetivos e o progresso de uma auditoria, a forma mais importante é o relatório formal. Os relatórios devem ajudar os auditados a compreender as questões de controle, recomendações e o risco associado de não tomarem medidas corretivas.

9.3.2.3 Valor do relatório

O valor do relatório reside na sua capacidade de comunicar o escopo, os objetivos, os resultados e as recomendações da auditoria. O valor reside também na capacidade do relatório de fornecer informações para persuadir e

auxiliar a alta administração da organização a reduzir riscos, atingindo objetivos organizacionais e tomando medidas corretivas. Para isso, o conteúdo do relatório deve ser compreensível para todos os usuários do relatório e ser apresentado em uma ordem lógica e um estilo legível.

O conteúdo do relatório deve ser suficientemente abrangente para permitir que o mesmo seja independente. O valor do relatório reside na capacidade do auditor de indicar claramente como a auditoria foi realizada, as descobertas e os benefícios de tomar medidas corretivas, se necessário for, e o risco ao não fazê-las.

O relatório pode cumprir outros objetivos, tais como servir como uma declaração de garantia do desempenho das operações, adequação dos controles internos ou a adequação das políticas e procedimentos de desenvolvimento dos sistemas.

Além disso, o relatório pode ser usado para auxiliar o gerenciamento de processos de negócios e o gerenciamento de SI na aquisição de recursos adicionais para apoiar iniciativas de TI.

O relatório pode ter um impacto significativo nas decisões de gestão relativas à organização auditada e aos seus destinatários. Dependendo do escopo e objetivos da auditoria, das conclusões e do parecer fornecido, as práticas de controle podem ser melhoradas, os recursos realocados e as medidas de desempenho recalibradas. Assim como o trabalho de auditoria deve ser realizado por pessoal de competente de acordo com as normas relevantes, a credibilidade do próprio trabalho de auditoria também depende de ter um relatório de auditoria bem escrito e devidamente organizado.

9.3.2.4 Tipos de relatórios de auditoria de SI

O relatório de auditoria de SI é direcionado principalmente pelo tipo de compromissos que a auditoria pretende cumprir. Antes de redigir o relatório, os auditores precisam estar familiarizados com os requisitos de relatórios das normas ISACA e quaisquer outros padrões de auditoria relevantes. Embora a maioria dos trabalhos de auditoria resulte em um único relatório, em algumas situações mais de um relatório pode ser aplicável. Por exemplo, além de um relatório para um público geral, um relatório confidencial separado contendo informações técnicas sensíveis pode precisar ser emitido

para garantir que as informações confidenciais não sejam disponibilizadas a partes não autorizadas.

A organização e o conteúdo específico do relatório também dependem do escopo e objetivos do trabalho de auditoria e do grau em que os processos e sistemas de TI são examinados ou exigem explicações. O formato e os protocolos para a apresentação do relatório também podem depender de quaisquer requisitos e expectativas estabelecidos entre a organização de auditoria e o auditado. Os requisitos para o conteúdo ou formato do relatório podem ser solicitados pelo cliente de auditoria que pode ou não ser da mesma parte que o auditado. Por definição, o cliente é a parte que mantém ou paga o auditor independente para realizar o trabalho de auditoria.

9.3.2.5 Tipos de compromissos de auditoria

Existem basicamente três tipos de compromissos de auditoria:

- ✖ **revisão** – uma revisão é projetada para fornecer garantia limitada sobre uma afirmação. Como o nome sugere, uma revisão consiste principalmente em trabalhos de revisão com menos ênfase em testes ou verificação. Uma revisão pode ser mais orientada para o processo, com foco na adequação das tarefas e atividades que a entidade de auditoria realiza e os controles associados. O nível de evidência coletado é menor do que em uma auditoria e o teste é geralmente limitado ou nenhum é realizado. Como resultado, as revisões não incluem opiniões de auditoria;
- ✖ **exame** – uma auditoria do sistema de informações pode ser realizada como um exame, que é um processo sistemático pelo qual uma pessoa competente e independente obtém objetivamente e avalia evidências sobre afirmações a respeito de uma entidade ou evento, processos, operações ou controles internos. A finalidade deste trabalho é formar uma opinião e fornecer um relatório sobre o grau em que as afirmações estão em conformidade com um conjunto identificado de normas. Um exame requer um limiar mais alto para evidências de auditoria do que uma revisão. Os testes de auditoria, por exemplo, podem se concentrar em uma comparação das práticas declaradas e atuais do auditado com padrões estabele-

cidos ou práticas de controle relevantes. Um relatório de auditoria pode fornecer três tipos de opiniões: não-qualificado, qualificado e adverso. O relatório de auditoria também pode emitir uma declaração de exoneração de responsabilidade indicando que, devido a certas circunstâncias (como a incapacidade de realizar um trabalho de auditoria suficiente ou obter evidência suficiente, relativa e válida), o auditor não pode tirar conclusões ou emitir parecer a respeito de um determinado processo;

- × **compromisso de procedimentos acordados** – em um compromisso de procedimentos acordados, um terceiro e o auditor concordam em procedimentos específicos que serão executados para obter a evidência em que o terceiro está disposto a basear-se como base para uma conclusão. Dependendo dos requisitos do terceiro, o nível de evidência acordado pode ser significativamente limitado ou extenso. O auditor pode precisar obter uma quantidade substancial de evidência em alguns casos. De acordo com a ISACA, o relatório de auditoria deve incluir uma declaração de que a suficiência dos procedimentos é exclusivamente de responsabilidade dos responsáveis. O relatório também deve indicar que se refere apenas aos elementos especificados e não se estende além destes.

9.3.2.6 Compromissos de Auditoria de SI

As auditorias de SI podem ser realizadas como uma revisão, exame ou compromisso de procedimentos acordados, mas podem ser categorizadas de várias maneiras. Embora as auditorias de SI tenham se concentrado cada vez mais em áreas altamente técnicas de TI, os compromissos de auditoria de SI incluem, mas não se limitam aos seguintes:

- × exame geral de controle ou auditoria de instalações;
- × auditoria de aplicações;
- × auditoria de desenvolvimento de sistemas;
- × auditoria de tópico técnico ou especial.

As **auditorias gerais de controle** são geralmente exames nos quais as práticas de controle de gestão e os controles gerais são avaliados quanto à ade-

quação de seu projeto e testados quanto à sua eficácia. As etapas de auditoria realizadas e as evidências obtidas servem de base para que os relatórios de auditoria incluam conclusões e opiniões.

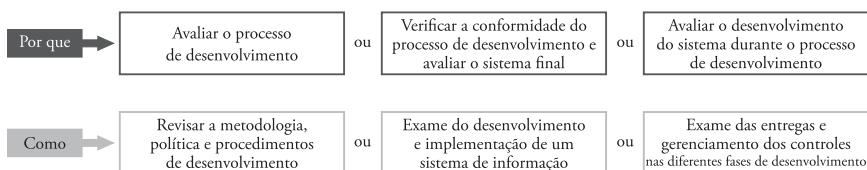
Embora as **auditorias de aplicativos** geralmente se concentrem na confiabilidade, segurança e disponibilidade do sistema, elas podem ser limitadas a um aspecto específico do sistema, como integridade de dados, armazenamento e recuperação de dados ou valor operacional. Do ponto de vista operacional, o escopo pode incluir uma avaliação de manutenção, controle de mudança e recuperação de desastres.

No domínio das **auditorias de desenvolvimento de sistemas**, os três tipos mais comuns de compromissos seguem descritos a seguir e também exemplificados na figura 9.3.

- ✖ Revisão da metodologia, política e procedimentos de desenvolvimento;
- ✖ Exame do desenvolvimento e implementação de um sistema de aplicação específico;
- ✖ Exame de entregas e controles de gestão em diferentes fases, à medida que o sistema está sendo desenvolvido;

O auditor também pode servir como consultor de controle ao longo do desenvolvimento e implementação do sistema de informações.

Figura 9.3 – Tipos de compromissos de auditoria de desenvolvimento de sistemas



Fonte: ISACA, 2015.

Embora seja possível que todos os tipos de compromissos de auditoria de desenvolvimento de sistemas incluam opiniões, é mais provável que o primeiro e o terceiro tipos tenham conclusões, devido ao trabalho de revisão orientada sobre o processo de desenvolvimento para cada uma das fases de desenvolvimento.

No segundo tipo apresentado é mais provável que contenha uma opinião, devido ao escopo e extensão do exame.

Embora a elaboração e emissão de relatórios de auditoria de sistema de informações seja geralmente realizada no encerramento do trabalho de auditoria, uma exceção a esta prática é durante o terceiro tipo de auditoria de desenvolvimento de sistema, quando mais de um relatório pode ser emitido. Dependendo da importância do sistema de informações, do tamanho do investimento, do risco associado e do período de tempo necessário para desenvolver e implementar o sistema, os relatórios de auditoria individuais referentes às fases de desenvolvimento podem ser emitidos.

As auditorias de tópicos técnicos ou especiais tendem a ter escopos mais limitados e objetivos de auditoria altamente técnicos. Esses compromissos geralmente são mais bem focados do que os exames de controle geral e podem ser realizados como revisões ou exames. Como tal, o conteúdo do relatório de auditoria depende da abrangência do escopo e dos objetivos da auditoria, da complexidade e da extensão do trabalho, das evidências, das explicações técnicas exigidas e das expectativas definidas dos usuários dos relatórios.

9.3.2.7 Identificação dos usuários do relatório

Um dos elementos-chave da comunicação é conhecer o público. Ao escrever um relatório de auditoria de SI, os interesses dos leitores e sua capacidade de entender o relatório precisam ser considerados. A seguir estão elencadas seis etapas (de “a” a “f”) que fornecem uma visão sobre o que o relatório precisa incluir de informações explicativas e detalhadas qualitativa e quantitativamente.

- a) Identificar os requisitos de conteúdo que são exigidos pelas normas profissionais de auditoria e pelas organizações de auditoria. Esta etapa fornece uma lista de tópicos obrigatórios, como título do relatório, escopo de auditoria e período de auditoria. Os leitores que estão familiarizados com os relatórios de auditoria procuram o conteúdo necessário;
- b) Identificar todas as categorias de leitores, desde a parte mais imediata que tem responsabilidade direta sobre a área ou entidade auditada até o leitor mais distante, que pode ser o público em geral. Esta etapa é usada como base para a análise do leitor e ajuda a determinar a distribuição do relatório;

- c) Determinar os interesses de cada categoria de leitor. Essa etapa garante que as informações apropriadas sejam incluídas e que o conteúdo útil não seja omitido;
- d) Identificar o impacto, em cada categoria de leitor, de um relatório que expresse uma opinião não qualificada, qualificada ou adversa. Esta etapa destaca a necessidade de informações explicativas ou texto persuasivo. Ela identifica quando instruções adicionais devem ser fornecidas ao solicitar respostas aos resultados da auditoria;
- e) Avaliar a capacidade das categorias de leitores para entender o material no relatório. Esta etapa impacta a necessidade de conteúdo explicativo e inclusão de material em um apêndice;
- f) Antecipar como cada categoria de leitor usará o relatório e as informações que ele contém. Grandes divisões sobre a capacidade de agir sobre os resultados do relatório podem enfatizar a necessidade de recomendar uma melhor comunicação e colaboração entre as principais partes.

Diferentes partes estão normalmente envolvidas em um processo operacional ou função que está sendo examinada. Desta forma, informações adicionais podem ser necessárias, tais como:

- ✗ para os leitores que não estejam familiarizados com os relatórios de auditoria, a finalidade do relatório deve ser claramente identificada na página de assinatura ou transmissão, introdução ou parágrafo de escopo;
- ✗ para os leitores que não estão familiarizados com os critérios de auditoria que estão sendo citados, é mais útil observar o valor ou a importância dos critérios, em vez de apenas visualizar uma lista de critérios;
- ✗ pode ser necessário incorporar orientações sobre como o leitor pode obter uma compreensão melhor dos critérios;
- ✗ para conteúdo da web, deve ser incluído informações adicionais ou uma cópia do material, porque o conteúdo da web não permanece constante;

- × se o relatório requer informações persuasivas adicionais, o auditor deve considerar a possibilidade de inserir resultados específicos de testes de auditoria, estimativas quantitativas do impacto da tomada ou não da ação, ou configuração de TI e detalhes operacionais. Além disso, deve considerar como apresentar um argumento convincente para persuadir os leitores que podem não concordar com o valor da ação corretiva.

A determinação da organização de **distribuição** de relatórios é a lista de partes a quem o relatório de auditoria final emitido será dirigido. A menos que a distribuição seja restrita, as cópias do relatório final são fornecidas à alta administração, aos membros da comissão de auditoria, aos proprietários de processos de negócios relevantes, às partes interessadas internas e externas e aos órgãos de supervisão. Os relatórios governamentais de auditoria de SI têm uma distribuição mais ampla, incluindo vias para divulgação pública, e podem estar disponíveis em um site governamental.

Recomenda-se que as listas de distribuição de relatórios sejam desenvolvidas no início do processo de envolvimento da auditoria para ajudar a assegurar que os leitores dos relatórios sejam adequadamente identificados e alinhados com a lista de indivíduos, organizações e grupos, como o público em geral.

9.3.2.8 Conformidade com as normas de auditoria

A divulgação dos resultados dos compromissos de auditoria requer o cumprimento das normas de auditoria, incluindo a *ISACA IS Audit and Assurance Standards*. Além de identificar os requisitos de relatório das normas profissionais de auditoria, os requisitos de relatório específicos da organização em questão e quaisquer leis ou regulamentos aplicáveis precisam ser identificados. Embora os requisitos de relatório que são estipulados por leis ou regulamentos devem ter precedência, a devida atenção profissional deve ser exercida no cumprimento das normas de auditoria e orientações relacionadas.

O auditor é responsável por assegurar que o trabalho de auditoria, incluindo relatórios, esteja em conformidade com as normas relevantes. Dependendo do tipo de auditoria, das políticas da organização e das certificações profissionais do auditor, podem ser aplicadas várias normas de auditoria.

9.3.3 Fase 2 – escrevendo o relatório

A fase 2 (escrevendo o relatório) consiste em observar os fatores de comunicação e fatores-chave de sucesso. Nesta fase é detalhado o conteúdo do relatório, sendo apresentado nos tópicos subsequentes.

9.3.3.1 Fatores de comunicação

Os relatórios de auditoria de sistemas de informação bem estruturados e claramente escritos promovem a credibilidade da auditoria e ajudam o leitor a compreender os pontos-chave de forma eficaz e eficiente. Os processos formais de elaboração de relatórios incorporam revisão e aprovação rigorosas, revisões de edição e exposição de relatórios preliminares aos auditados. A informação no relatório de auditoria de SI precisa ser verificável e apresentada de forma construtiva e imparcial.

Ao elaborar um projeto de relatório, torna-se rapidamente evidente que a qualidade dos documentos de trabalho de auditoria afeta significativamente a capacidade do auditor de redigir o relatório. Relatórios bem escritos são geralmente o produto de documentos de trabalho de auditoria adequadamente documentados. Começar com o planejamento e progredir por meio do processo de auditoria é a oportunidade contínua de identificar os interesses e os requisitos de comunicação dos leitores mais imediatos do relatório. Esta avaliação permite uma melhor determinação da linguagem que será utilizada, a necessidade de definir a terminologia e o grau de explicação exigido no relatório.

9.3.3.2 Fatores-chave de sucesso

Além de relatar os resultados da auditoria, o relatório de auditoria de SI tem como objetivos fornecer garantias, informar auditados e outros sobre questões de gerenciamento e controles, recomendar ações corretivas e representar a qualidade e credibilidade da organização de auditoria. A forma como o relatório é organizado e escrito pode impactar significativamente nestes objetivos. O relatório deve ajudar as partes responsáveis na compreensão de questões complexas, melhorar o controle e o desempenho, gerenciar riscos e promover boas práticas e soluções. Os relatórios são um veículo importante para informar a administração da entidade auditada e outras partes sobre as

melhores práticas de governança, gestão e controle. Também deve ajudar o leitor a entender a relação entre os objetivos da auditoria, os objetivos operacionais e de controle da entidade auditada e, as conclusões relacionadas com a auditoria.

× **Informativo**

O relatório deve ser escrito de forma clara, concisa e persuasiva. Deve ser informativo, equilibrado e apresentado usando linguagem e tom que promovam a capacidade de compreendê-lo. O relatório deve ser profissionalmente apresentado em termos de estrutura, formato, facilidade de encontrar informações e estilo de escrita. Também deve estar bem organizado e bem escrito e apresentar os resultados da auditoria de forma equilibrada, justa e objetiva.

× **Sequência lógica**

Para ser claro e conciso, o relatório deve apresentar o material em uma sequência lógica. Conciso implica que palavras e frases são diretas, sendo que as frases não são excessivamente prolixas ou muito demoradas. O auditor pode ler o relatório em voz alta e ouvir como ele soa, determinar se está livre de frases difíceis, e decidir se muitas respirações precisam ser tomadas para completar a frase.

Embora o relatório de auditoria possa apresentar o material em uma sequência lógica e de uma forma concisa, pode ser necessário ser demorado para cobrir adequadamente a auditoria e seus resultados. Ao escrever o relatório, o auditor deve considerar se os leitores são aptos a gastar tempo metodicamente na leitura e estudo do relatório. Se o relatório for longo e contiver questões complexas, um resumo executivo pode ser inserido na parte da frente do relatório para ajudar o leitor a identificar e compreender as mensagens mais importantes. Um resumo executivo geralmente não é necessário para relatórios curtos e concisos.

× **Persuasivo**

Para ser persuasivo, o relatório precisa ser convincente. Ele precisa apresentar argumentos para a ação de forma que o leitor compre-

enda a importância de tomar medidas e o risco que assumirá caso não agir. A maneira pela qual um achado de auditoria é apresentado também ajuda o auditor a ser persuasivo, porque apresenta o argumento para a ação corretiva logicamente e informativamente. Ao apresentar um problema ou deficiência e uma recomendação desta maneira, ele pode ajudar a persuadir a entidade auditada a iniciar ações corretivas.

O auditor deve considerar maneiras que a informação pode ser apresentada para ajudar o leitor a compreender os pontos-chave do argumento. A utilização de tabelas, gráficos de pizza, gráficos de barras e outros gráficos para transmitir informações adicionais deve ser considerada. Embora a regra geral seja usar cores de maneira moderada, deve-se considerar o uso de cores com diferentes fontes e estilos de fonte (negrito, itálico, sublinhado) para chamar a atenção para elementos chave ou destacar informações.

✗ **Informações suficientes**

Para determinar se um relatório é informativo, deve-se considerar se o mesmo fornece explicações suficientes. Para ajudar a tomar essa decisão, as seguintes perguntas podem ser feitas:

- ✗ qual é o conhecimento do leitor sobre o assunto?
- ✗ até que ponto os leitores do relatório já conhecem as questões?

Mesmo indivíduos que estão muito familiarizados com as operações da organização auditada podem não ter conhecimento de alguma parte do relatório. Portanto, as informações de fundo adicionadas podem aumentar o valor do relatório. Deve-se também considerar o benefício do uso de informações adicionais ou suplementares. Fornecer referências ou cópias de informações suplementares em um apêndice muitas vezes pode ajudar o leitor a obter uma melhor compreensão do material do relatório.

9.3.3.3 Comprimento e conteúdo

O comprimento e o conteúdo de um relatório de auditoria de SI dependem dos seguintes fatores:

- × requisitos predefinidos que são exigidos pelas normas de auditoria;
- × requisitos adicionais que são ditados pelas necessidades de classes diferenciadas de leitores;
- × complexidade do material;
- × protocolos de relatórios que são estabelecidos pela organização de auditoria.

Os fatores que afetam o conteúdo do relatório incluem os seguintes:

- × tipo de auditoria;
- × complexidade de operações e sistemas da entidade auditada;
- × número de objetivos e achados de auditoria;
- × diferentes categorias de leitores;
- × detalhes necessários para tornar o conteúdo comprehensível;
- × divulgações;
- × informações complementares necessárias.

Os relatórios de auditoria que são disponibilizados ao público provavelmente conterão uma explicação mais detalhada das operações e objetivos do negócio do que os relatórios de auditoria interna que são submetidos exclusivamente aos gestores.

9.3.3.4 Conteúdo do relatório

As normas de auditoria estipulam que os relatórios contenham ao menos alguns tópicos. A estrutura do relatório, a ordem de apresentação, a terminologia e a formatação apropriadas impactam os objetivos para tornar os relatórios legíveis e comprehensíveis. Por exemplo, a utilização de títulos com termos reconhecidos e diferentes tamanhos de fonte ajudam a tornar a informação do relatório facilmente distinguível e ajudam o leitor a navegar pelo relatório. A maioria dos relatórios de auditoria incluem as seguintes seções principais.

- a) Página de título (a identificação do relatório é obrigatória);
- b) Página signatária e de transmissão (a assinatura é obrigatória);

- c) Índice (opcional);
- d) Introdução (opcional);
- e) Resumo executivo (opcional dependendo da duração e complexidade do relatório);
- f) Âmbito da auditoria (obrigatório);
- g) Objetivo(s) da auditoria (obrigatório);
- h) Metodologia da auditoria (obrigatório);
- i) Resultados da auditoria (obrigatório);
- j) Conclusão ou opinião da auditoria (obrigatório);
- k) Recomendações (obrigatório);
- l) Resposta da administração (obrigatório);
- m) Resposta do auditor (opcional);
- n) Apêndice (opcional).

9.3.3.5 Modelo de relatório

A seguir o exemplificaremos um modelo básico de relatório de auditoria de SI.

a) Folha de rosto

As seguintes informações devem ser incluídas na folha de rosto:

- × rubrica intitulada “Relatório do Auditor Independente”;
- × nome da organização de auditoria;
- × título do relatório;
- × nome da entidade de auditoria;
- × período de auditoria coberto pela auditoria.

b) Página do signatário

A página do signatário é geralmente apresentada em papel timbrado da organização de auditoria. Ela identifica o que a organiza-

ção de auditoria está apresentando em termos de relatório. O texto identifica a auditoria, o período em que o trabalho de auditoria foi realizado e a data da emissão do relatório e indica que o relatório contém conclusões e/ou opiniões. A página do signatário serve como uma página de transmissão quando o relatório de auditoria é formalmente transmitido da organização de auditoria para o auditado e, se necessário, a um cliente.

c) Índice

O auditor deve considerar a inserção de um índice para ajudar os leitores a localizar informações ao longo do relatório de auditoria.

d) Introdução

Embora uma introdução separada não seja um elemento obrigatório de um relatório de auditoria, ela pode melhorar a capacidade de compreender os relatórios que serão lidos por indivíduos que não estão familiarizados com a entidade de auditoria ou o sujeito da auditoria. A seção de introdução fornece aos leitores externos informações suficientes sobre o tipo de entidade de auditoria, sua missão e objetivos primários de negócios, e a finalidade dos sistemas de aplicativos e tecnologias de suporte que estavam sujeitas a auditoria.

e) Resumo executivo

Um resumo executivo é uma excelente maneira de apresentar informações resumidas se os relatórios são longos e/ou complexos. Embora um resumo executivo possa ser usado para persuadir a gerência a tomar medidas corretivas, não deve ser usado para criar alarde quanto aos resultados da auditoria. Em vez disso, deve ser informativo e direto ao ponto.

f) Escopo da auditoria

O escopo da auditoria é uma declaração do sujeito da auditoria. Essencialmente, o tipo de auditoria e o que está a ser auditado. O escopo da auditoria identifica a autoridade para realizar a auditoria, o nome da organização e da entidade de auditoria e o período coberto por ela.

Para um leitor experiente, o escopo da auditoria deve indicar a amplitude esperada do trabalho e as áreas de tópico cobertas pela auditoria.

g) Objetivos da auditoria

A seção de objetivos identifica os itens a serem avaliados pela auditoria. Dependendo do escopo, vários objetivos podem ser identificados. É importante notar que estes são objetivos de alto nível e não objetivos detalhados relacionados a procedimentos específicos. O auditor precisa considerar se os objetivos podem ser apresentados em termos hierárquicos, apresentando primeiro o objetivo de auditoria principal com objetivos secundários a serem seguidos. Sugere-se que sejam utilizados parágrafos separados para agrupar os objetivos superior e secundário.

h) Metodologia de auditoria

A metodologia de auditoria deve fornecer uma explicação de alto nível sobre como a auditoria foi realizada para cada objetivo. A metodologia deve identificar a natureza e a extensão do trabalho, os critérios, as fontes de critérios, a dependência do trabalho de outros profissionais, o tipo de análise realizada e a base para as conclusões. A explicação da metodologia fornece ao leitor uma compreensão dos procedimentos que foram realizados para obter a evidência que era necessária para abordar os objetivos da auditoria e a natureza subsequente da garantia que é transmitida pelo relatório de auditoria.

i) Conclusão ou opinião de auditoria

O objetivo desta seção é fornecer uma conclusão geral ou parecer com relação aos objetivos do trabalho de auditoria. Para auditorias que atendam aos requisitos de obtenção de evidências suficientes, relevantes e confiáveis e tenham cumprido outras normas de auditoria, os relatórios geralmente incluem uma opinião ou um aviso de isenção de responsabilidade.

j) Resultados da auditoria

O objetivo desta seção é fornecer uma explicação mais detalhada dos resultados da auditoria encontrados. A conclusão geral ou opinião determina se o relatório deve conter uma seção de resultados.

Se o relatório conter uma opinião não qualificada, então é impróprio que os resultados da auditoria sejam incluídos. Para relatórios contendo opinião qualificada ou adversa, os resultados da auditoria devem ser incluídos.

9.3.3.6 Construindo relatórios de auditoria de SI bem escritos

Um bom relatório de auditoria contém fatos precisos e concisos que são facilmente compreendidos pelos leitores. Além de terminologia, linguagem, estrutura de relatório, requisitos de conteúdo e protocolo, estrutura de sentenças e pontuação também são considerados importantes. Devem ser observadas as regras de boa escrita da língua portuguesa.

9.3.3.7 Processo de rascunho do relatório

Ao adotar um modelo definido, os auditores podem começar a preencher o rascunho à medida que a auditoria prossegue, após finalizar o planejamento da auditoria ou a fase de auditoria prospectiva. Neste ponto, os auditores definiram e obtiveram revisão e aprovação do escopo da auditoria, período, objetivos e estratégia de auditoria. Portanto o rascunho pode ser escrito à medida que os trabalhos de auditoria avançam.

9.3.4 Fase 3 – finalizando o relatório

A fase 3 (finalização do relatório) consiste em informações adicionais, edição final, revisão, aprovação e redação dos eventos subsequentes à auditoria.

9.3.4.1 Incluindo Informações Adicionais

Durante esta fase, informações adicionais serão incluídas no relatório de auditoria. Como o relatório preliminar formal não incluiu as respostas da administração às conclusões da auditoria, esta informação é inserida neste momento. Além disso, se necessário, as respostas do auditor são incluídas para reconhecer as ações corretivas que foram tomadas ou estão planejadas, ou identificar quaisquer resultados ou recomendações no relatório de auditoria que as respostas da administração não abordaram. Outras informações adicionais incluem uma descrição de eventos subsequentes que podem ser

relevantes para a auditoria, itens a serem inseridos em um apêndice e quaisquer divulgações adicionais.

9.3.4.2 Edição final, revisão e aprovação

Uma vez que o trabalho de auditoria e o projeto final de relatório que foi submetido à entidade auditada já foram submetidos à revisão e aprovação da alta administração, é improvável que sejam necessárias alterações extensivas a serem reportadas. No entanto, se novas informações foram adicionadas ao finalizar o relatório e, dependendo do feedback recebido do auditado, certas partes do relatório podem precisar ser reescritas para fortalecer o mesmo. Depois que as informações adicionais forem incluídas e quaisquer alterações forem feitas, o relatório deve ser sujeito a uma revisão final pela alta gerência de auditoria antes que seja emitido definitivamente.

9.3.4.3 Eventos subsequentes

O relatório final deve incluir informações relativas a quaisquer eventos que ocorreram após o trabalho de campo da auditoria ter sido concluído. Embora o auditor não seja responsável pela detecção de eventos subsequentes, é aconselhável perguntar ao administrador da organização se existiram tais eventos, e se podem ser relevantes para o assunto da auditoria. Mesmo que a integridade do trabalho de auditoria, incluindo conclusões e expressão de opiniões, não seja diminuída por eventos subsequentes, a divulgação destes e o ajuste junto ao conteúdo do relatório, especialmente em relação às recomendações, aumenta a utilidade do relatório final de auditoria.

Síntese

Aplicar técnicas e melhores práticas já consolidadas no mercado para o trabalho de auditoria é fundamental para que haja efetividade no trabalho do auditor, bem como produzir resultados relevantes para a organização. Neste capítulo aprendemos quais são estas técnicas e melhores práticas, bem como o que um bom relatório de auditoria deve conter.

As três fases do relatório, preparação, escrita e finalização, contemplam diversas etapas que devem ser observadas pela equipe de auditoria para que o relatório produza os efeitos esperados definidos antes do início do trabalho de auditoria.

Atividades

1. Quanto à técnica de inserção de dados de teste, analise a seguinte frase e responda se está correta: *“esta técnica também é conhecida como test data ou test deck e envolve o uso de um conjunto de dados especialmente projetados e preparados com o objetivo de testar as funcionalidades de saída de dados no sistema”.*
 - a) Certo
 - b) Errado
2. A fase de entrevistas é parte fundamental do processo de auditoria. Explique, resumidamente, a diferença entre entrevistas diretivas e não-diretivas.
3. A etapa de conformidade com as normas de auditoria estabelece que o relatório deve estar alinhado com normas atuais, como por exemplo a *“ISACA IS Audit and Assurance Standards”*. Esta etapa está inserida na fase de:
 - a) Preparação
 - b) Escrita
 - c) Finalização
4. “Fornecer declarações de segurança e, se necessário, identificação de áreas que requerem ações corretivas e recomendações relacionadas” é um dos seis objetivos principais do relatório de auditoria.
 - a) Certo
 - b) Errado

10

Ferramentas de Auditoria de Sistemas de Informação

NESTE CAPÍTULO SERÃO apresentadas ferramentas que auxiliam no trabalho de auditoria de sistemas de informação, com foco em ferramentas generalistas. Tais ferramentas auxiliam o trabalho do auditor, capturando as informações de diversas bases de dados e apresentando-as de forma a facilitar sua análise, bem como a apresentação de relatórios.

Objetivo de aprendizagem:

- × Conhecer algumas ferramentas de apoio à auditoria de sistemas de informação.

10.1 Classificação das ferramentas para auditoria de sistemas de informação

As ferramentas de auditoria de sistemas são os meios que auxiliam o auditor a atingir seus objetivos, previamente definidos no planejamento inicial de auditoria, seja qual for a natureza da auditoria praticada. Via de regra, as ferramentas que serão utilizadas em um trabalho de auditoria interna serão norteadas pelos instrumentos definidos e aplicados nas etapas de auditoria externa.

Lyra (2008), classifica as ferramentas disponíveis no mercado em três categorias básicas, e apresenta também alguns exemplos de softwares utilizados, sendo elas: ferramentas generalistas, ferramentas especializadas, e ferramentas de uso geral. Apresentaremos nos tópicos a seguir tais ferramentas, de modo que possamos conhecer mais a fundo as funcionalidades destas.

10.2 Ferramentas generalistas de auditoria de SI

As ferramentas generalistas, segundo Lyra (2008), são softwares que podem processar, simular, analisar amostras, gerar dados estatísticos, summarizar, apontar duplicidades e outras funções que o auditor desejar. As principais vantagens do uso destas ferramentas residem no fato de que tais aplicativos podem processar vários arquivos ao mesmo tempo, bem como processá-los em vários formatos. Também podem ser integrados de forma sistêmica com diferentes outros softwares e plataformas (hardwares). Outra vantagem é reduzir a dependência do auditor quanto a especialistas em Tecnologia da Informação.

Entre as desvantagens inerentes ao uso de ferramentas generalistas, podemos citar a impossibilidade de execução de cálculos complexos, além da limitação quanto ao uso em ambiente on-line.

A seguir faremos a apresentação de algumas destas ferramentas generalistas.

10.2.1 ACL (Audit Command Language)

Tal software é desenvolvido por uma empresa de mesmo nome, com sede na cidade de Vancouver, no Canadá. O software permite analisar dados em quase qualquer formato de praticamente qualquer plataforma, mesmo quando trata-se de grande quantidade de dados.

A tomada de decisões eficaz depende do acesso oportuno às informações. Essas informações podem estar ocultas em grandes arquivos de dados, espalhados em vários bancos de dados ou armazenados em uma variedade de tipos de dados em diferentes plataformas. Os tomadores de decisão e analistas de dados precisam de ferramentas que podem ajudá-los a acessar vários tipos de dados, processar arquivos grandes e fazer perguntas inteligentes sobre os dados.

Por muito tempo a análise de dados tem dependido de métodos estatísticos. Embora as estatísticas permitam fazer generalizações úteis sobre os dados, eles dependem da amostragem e analisam apenas uma pequena porcentagem do total de registros. Softwares convencionais, como planilhas eletrônicas, analisam apenas um número limitado de registros que foram convertidos em um formato que o aplicativo pode reconhecer. Por isso os auditores necessitam de ferramentas que possam ler e analisar dados de qualquer forma e de qualquer ambiente, além de serem capazes de acessar dados de várias fontes ao mesmo tempo e estar livre de limitações de tamanho de arquivo.

O software ACL fornece acesso a praticamente qualquer fonte de dados, na maioria dos casos sem preparação antecipada ou conversão. O auditor pode prontamente realizar consultas e manipulação de dados em arquivos que exigiriam preparação manual extensa e conversão com outros softwares de análise. É possível também, através desta ferramenta, a combinação de dados de sistemas diferentes para conversão, reconciliação e controle. Também pode ser um componente utilizado na integração de sistemas, de modo a permitir criar uma visão comum de dados em arquivos diferentes e analisá-lo como se existisse em um arquivo.

10.2.1.1 Leitura dos dados pelo software ACL

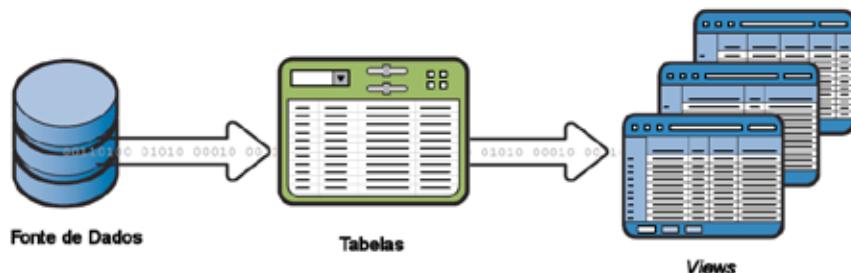
O software ACL usa tabelas para descrever o local, o layout e o conteúdo dos dados de origem. O auditor cria *views* para exibir dados em suas tabelas,

podendo também criar várias visualizações para cada tabela. Existem duas formas de criar uma nova tabela:

- × usando o assistente de definição de dados;
- × definindo dados manualmente;

O auditor pode editar o layout da tabela mais tarde para adicionar, excluir ou modificar os campos que deseja analisar. Também pode copiar, vincular e compartilhar tabelas entre projetos. A figura a seguir exemplifica a leitura de dados pelo ACL:

Figura 10.1 – Leitura dos dados pelo software ACL



Fonte: Elaborada pelo autor.

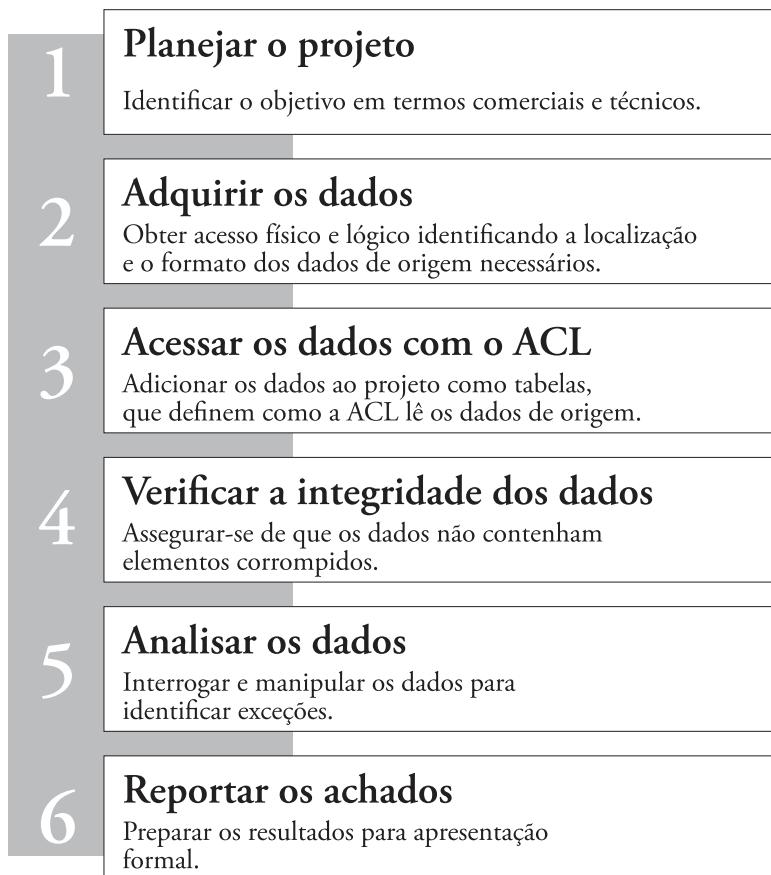
Saiba mais

O software possui várias formas de acessar os dados, mais informações podem ser obtidas no menu Help >> *accessing data*.

10.2.1.2 Fases de um projeto ACL

Via de regra, um projeto de auditoria desenvolvido no software ACL envolve seis fases: planejar, adquirir, acessar, verificar integridade, analisar e reportar. Tais fases são detalhadas na figura a seguir, bem como nos tópicos subsequentes:

Figura 10.2 – Fases de um projeto ACL



Fonte: Adaptada de <http://www.acl.com>.

10.2.1.3 Planejar o projeto

Os auditores podem começar o projeto com uma caneta e papel escrevendo de forma clara e inequívoca as declarações dos objetivos do projeto. À medida que articulam seus objetivos específicos, isto traz clareza adicio-

nal para o processo. Podem ser escritos vários desses objetivos, sendo que as declarações objetivas são específicas, em vez de gerais.

Devem ser identificados os processos a serem auditados e as informações que esperam descobrir. Por exemplo, um objetivo do projeto poderia ser: “identificar fornecedores cobrando mais do que os montantes acordados inicialmente”. Quanto mais específico mais facilmente será esclarecido os passos a fim de alcançar o objetivo.

Estes objetivos também influenciam os requisitos técnicos do projeto. Caso o auditor deseje incluir certas informações no relatório final, deve verificar se esses campos de dados estão presentes nos dados adquiridos para o projeto.

Com as declarações objetivas prontas, o auditor poderá determinar as etapas técnicas que irão apoiá-lo na realização de seus objetivos. Isso pode ser um processo iterativo, pois os requisitos técnicos podem depender da disponibilidade de arquivos ou campos de dados. A avaliação técnica geralmente inclui essas atividades:

- × **avaliar a viabilidade** – com base nas declarações objetivas, que identificam o tipo de informação (entrada) e o resultado desejado (saída), é possível determinar se o tipo de análise é viável. Pode haver casos em que há dados insuficientes para realizar os objetivos.
- × **identificar os arquivos de dados necessários** – identificar quais arquivos de dados contêm os campos de dados necessários aos trabalhos. Por exemplo, para comparar o preço contratual de um fornecedor com o preço da fatura, pode ser preciso o acesso a arquivos com preços contratuais, bem como faturas com detalhes de cada produto. Também pode ser preciso mais de um arquivo de dados para obter todos os campos necessários.
- × **certificar-se da possibilidade de armazenar os arquivos de dados** – o auditor deve estimar o máximo possível o tamanho aproximado dos dados solicitados. Deve também considerar o meio no qual receberá os dados e a capacidade do servidor de rede ou unidade de disco local.

Com todos os elementos no lugar, será possível planejar como realizar cada objetivo. Isso envolve a especificação dos dados de origem, comandos, expressões e variáveis que serão empregadas.

O cumprimento de um objetivo pode exigir mais de um passo, de modo que uma abordagem detalhada passo a passo deve ser articulada e revisada antes do início. Isso ajudará a garantir que não ocorrem eventos inesperados durante o processamento e que todos os resultados possíveis tenham sido levados em consideração. Também apresentará um panorama abrangente que permite identificar processos que podem ser executados de forma mais eficiente com outras funcionalidades. Por exemplo, executar a comparação de preços unitários para o exemplo de auditoria do fornecedor pode envolver as seguintes etapas:

- ✖ criar uma relação entre a tabela de detalhes da fatura e a tabela de inventário com o número do produto como o campo chave;
- ✖ criar um campo que revele a porcentagem de sobrepreço, ou seja, preço acima de um valor considerado normal, para cada produto na tabela de fatura em comparação com o preço unitário padrão;
- ✖ executar o comando no sistema ACL denominado “estatísticas” neste campo para obter informações gerais sobre as características da porcentagem de sobrepreço;
- ✖ criar um campo calculado que revele o valor total em reais do sobrepreço para cada transação;
- ✖ executar o comando “estatísticas” neste campo para obter informações gerais sobre as características do sobrepreço;
- ✖ executar o comando “classificar” no código do fornecedor, organizando este campo para determinar a distribuição do sobrepreço pelo fornecedor.

10.2.1.4 Adquirir os dados para o projeto

Dependendo da análise que será executada, o auditor pode ter que depender de outros entes para fornecer os dados de que necessita.

Os dados de origem podem estar em um computador *mainframe*, um minicomputador ou um computador pessoal. Podem ter qualquer estrutura de registro, uma variedade de tipos de dados e podem estar em disco rígido, *pendrives* ou outros dispositivos de armazenamento que podem ser lidos por seu computador pessoal.

Para obter os arquivos e layouts necessários para o projeto, o auditor deve fazer um pedido abrangente de dados. Os layouts de arquivos devem conter as seguintes informações.

- × Nome do arquivo de dados;
- × Tamanho do registro;
- × Nome do campo;
- × Posição inicial do campo;
- × Tamanho do campo;
- × Tipo de campo;
- × Formato do campo;
- × Descrição do campo.

Saiba mais

Usar conexão do tipo ODBC para acessar os dados está entre as maneiras mais fáceis de recriar um banco de dados, pois o software ACL pode criar automaticamente uma tabela utilizando-se deste método.

A tabela a seguir exemplifica um tipo de layout de arquivo:

Tabela 10.1 – Tipo de layout de arquivo

Nome do Campo	Posição Inicial	Tamanho	Tipo	Formato	Descrição
NroProduto	1	7	Caractere		Número do Produto

Nome do Campo	Posição Inicial	Tamanho	Tipo	Formato	Descrição
DescProduto	8	20	Caractere		Descrição do Produto
PrecoUn	28	6	Numérico	9.999,99	Preço Unitário
PrecoDt	34	10	Data	dd/mm/yyyy	Data do Preço

10.2.1.5 Acesso aos dados do projeto

Antes de trabalhar com um novo arquivo de dados, o auditor necessita informar ao software ACL como ler e interpretar os dados que ele contém. Isto é feito adicionando tabelas ao projeto no ACL. O layout de uma tabela descreve a estrutura e o conteúdo dos dados de origem e especifica onde os dados de origem podem ser encontrados. Também descreve os dados em cada campo, identifica os campos que serão analisados e como exibir e imprimir essas informações.

Existe uma funcionalidade denominada *Assistente de Definição de Dados*, que facilita a criação de tabelas para todos os tipos de dados comuns.

Os itens associados a um projeto ACL incluem:

- ✗ tabelas;
- ✗ *views*;
- ✗ *scripts*;
- ✗ índices;
- ✗ logs de comando;
- ✗ pastas.

Um projeto de ACL é como um armário de arquivos, sendo usado para armazenar todos os itens de projeto relacionados, como tabelas, visualizações, scripts, índices, logs e pastas. Para cada fonte de dados que será analisada, é necessário adicionar uma nova tabela ao projeto ACL.

A versão *Server Edition* traz um avanço significativo no acesso aos dados armazenados em servidores. Entre as vantagens, destacam-se:

- × leitura de arquivos diretamente do servidor;
- × opção de processar arquivos no cliente ou no servidor;
- × vários usuários do ACL podem acessar o servidor simultaneamente;
- × utilização do poder de processamento do servidor.

10.2.1.6 Verificação da integridade dos dados

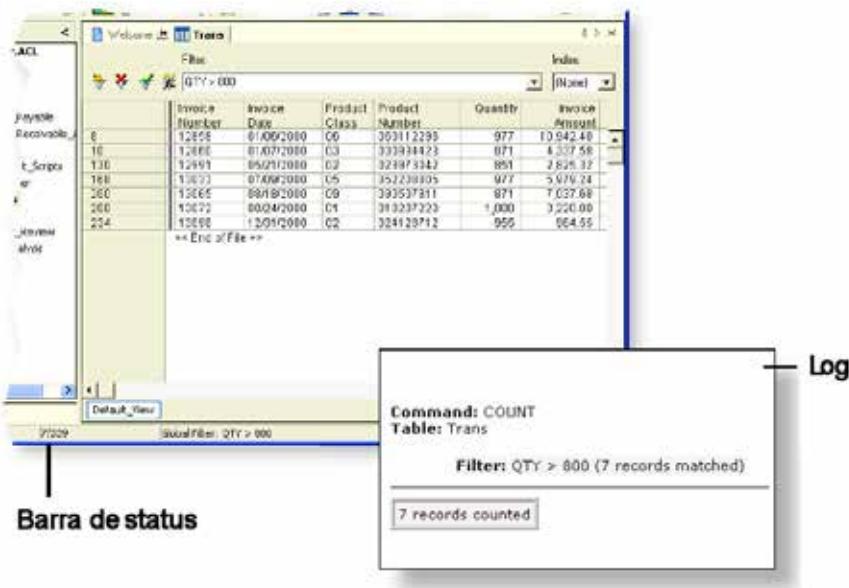
Uma das primeiras tarefas na análise de dados é garantir que se tenha dados completos e válidos. A verificação é especialmente importante quando se trabalha com arquivos de dados que não contêm informações sobre seu próprio *layout* de registro.

É possível usar testes como contagem de registros, totalização de campos e verificação de dados para garantir que:

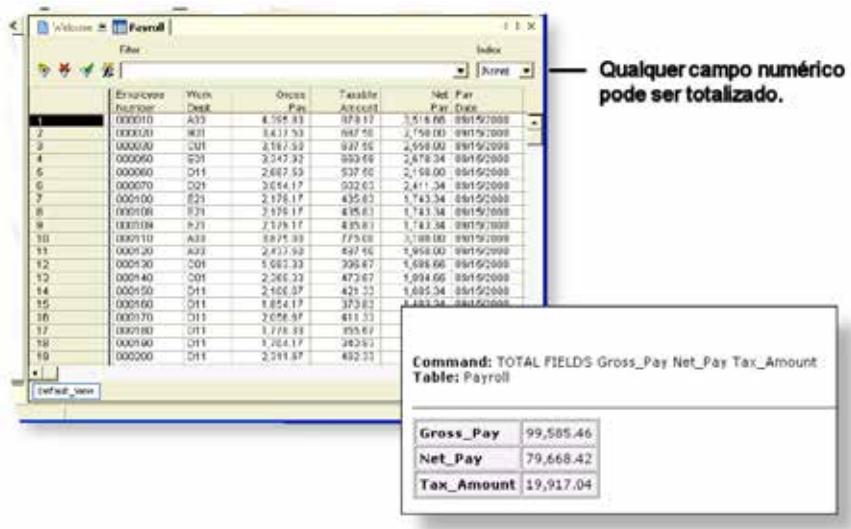
- × os arquivos contêm o número correto de registros;
- × os totais numéricos correspondem aos totais de controle fornecidos pelo proprietário do dado;
- × os campos contêm apenas dados válidos.

O software possui um comando denominado *Count* para contar o número de registros na tabela ativa ou apenas aqueles que atendem a uma condição de filtro especificada. Cada vez que é utilizado este comando o software ACL salva o resultado no log de comando e exibe-o na barra de status. Se for aplicado um filtro de exibição, o comando irá mostrar o número total de registros na exibição. A figura a seguir apresenta um exemplo de uso do comando.

Figura 10.3 – Comando Count



Existe também um comando denominado *Total*, que serve para totalizar campos numéricos ou expressões na tabela ativa. É possível usar o comando para provar a integridade e a precisão dos dados e produzir totais de controle. O comando localiza a efetua a soma aritmética dos campos ou expressões especificadas. A figura a seguir apresenta um exemplo de uso do comando.

Figura 10.4 – Comando *Total*

A etapa de verificação dos dados de uma tabela, se estão em conformidade com o layout definido anteriormente, é feita por meio do comando *Verify*. Todos os campos definidos podem ser analisados para garantir que os dados sejam consistentes com o tipo de dados de cada campo conforme especificado na definição de dados.

10.2.1.7 Análise dos dados do projeto

O software ACL funciona com uma tabela de cada vez. No entanto, é possível trabalhar com várias tabelas de várias maneiras: anexando uma tabela a outra, mesclando ou juntando-as em uma única tabela nova ou relacionando tabelas entre si para que possam ser analisadas como se fossem uma única tabela. Uma vez que os dados de várias tabelas estão relacionados ou combinados por junção, mesclagem ou anexação, a tabela resultante pode ser analisada com qualquer um dos comandos do ACL. Os comandos principais incluem funções de:

- ✗ resumo de dados;
- ✗ exame de dados sequenciais;

- × localização e análise isolada de registros;
- × classificação e indexação;
- × relacionamentos entre tabelas;
- × análise por amostragem.

10.2.1.8 Relatório dos achados

Nesta etapa são gerados relatórios baseados em vários modos de exibição, de acordo com os resultados obtidos nas etapas anteriores. O software permite a geração de diversos tipos de relatórios em planilhas, gráficos e outras formas interativas, utilizando-se de modelos previamente estabelecidos.

10.2.2 IDEA (Interactive Data Extraction & Analisys)

O software IDEA, produzido pela empresa Caseware, é uma ferramenta versátil e de fácil utilização, projetada para ajudar os profissionais de auditoria a ampliar seus recursos, detectar fraudes e atender aos padrões de documentação. O software facilmente importa dados de quase qualquer fonte para analisar grandes conjuntos de dados, auxiliando na análise e apresentação de relatórios usando ferramentas de visualização, bem como efetua automatização de processos repetitivos sem necessidade de programação.

10.2.2.1 Visão geral do software IDEA

O software usa projetos para organizar os arquivos a serem auditados. Um projeto é um tipo de recipiente usado para armazenar um conjunto de arquivos originais, que compõem os dados importados de um cliente e quaisquer arquivos subsequentemente gerados por meio de análise. O IDEA permite criar dois tipos de projetos de área de trabalho local: gerenciado e externo.

Os manuais do software recomendam que os arquivos de dados para cada auditoria ou investigação sejam armazenados em pastas separadas para simplificar o gerenciamento e a limpeza de bancos de dados e outros arquivos associados à auditoria ou investigação.

A ferramenta oferece a capacidade de importar quantidades massivas de dados de fontes diversas, incluindo sistemas ERP, planilhas, *mainframes* com sistemas legados, arquivos impressos, entre outros.

Existem modelos pré-determinados que auxiliam o auditor a criar automaticamente gráficos e estatísticas de análise. A figura a seguir apresenta um exemplo de apresentação gráfica de resultados que pode ser obtida através da utilização da ferramenta.

Figura 10.5 – Relatórios do sistema IDEA



O software IDEA inclui uma ferramenta de desenvolvimento conhecida como *IDEAScript* para criar macros a fim de estender a funcionalidade do IDEA. O script pode ser pronto, escrito a partir do zero, ou uma combinação de ambos.

O código é gerado ou escrito na janela *IDEAScript*. Esta janela tem uma barra de ferramentas que fornece acesso a um número de opções e ferramentas comumente usadas para auxiliar na escrita, edição e depuração de macros.

A partir da versão oito, é possível criar macros por meio de um recurso chamado *Visual Script*. Este recurso é usado para criar visualmente, editar e manter macros. O benefício do *Visual Script* é que ele per-

mite automatizar tarefas que são executadas repetidamente sem escrever qualquer código ou programação.

Quando um projeto novo é criado, o IDEA cria subpastas de biblioteca que permitem organizar todos os arquivos de projeto associados. Há três bibliotecas disponíveis no IDEA:

- ✖ **biblioteca corporativa** – um repositório de arquivos no servidor IDEA compilado por profissionais especializados. A biblioteca corporativa contém os grupos de biblioteca padrão do sistema;
- ✖ **biblioteca local** – um repositório de arquivos na unidade local que é utilizado para compartilhar arquivos com todos os projetos em andamento;
- ✖ **biblioteca de projeto atual** – um repositório de arquivos para o projeto ativo, bem como o projeto do servidor IDEA vinculado, se aplicável.

10.2.3 Pentana

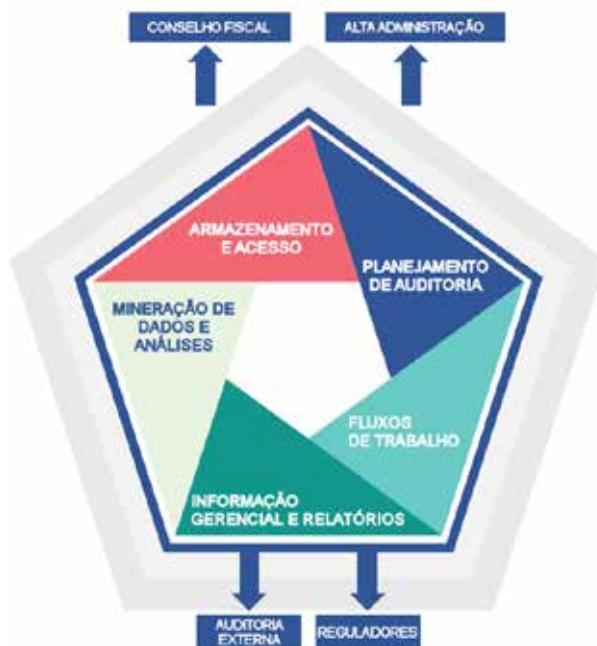
Pentana é um software de planejamento estratégico de auditoria. O foco do produto é oferecer uma solução completa para auditoria baseada em gestão de risco, por meio de governança organizacional e alto desempenho operacional. As equipes de auditoria em empresas reguladas precisam de visibilidade dos riscos atuais e emergentes em todas as áreas da organização para gerenciar esses riscos, garantir a conformidade e evitar falhas, ao mesmo tempo em que conectam a estratégia de negócios ao desempenho operacional. O Pentana impulsiona a conformidade e oferece *insights* em tempo real sobre o perfil de risco da organização e o status dos controles financeiros e de gerenciamento.

Outro objetivo do produto é capacitar o departamento interno de auditoria para ser mais produtivo, direcionar conformidade, gerenciar riscos e fornecer informações de gerenciamento de alta qualidade. Para isso o software auxilia a implementar uma metodologia consistente e compatível com as normas internacionais de risco e auditoria, integrando todos os aspectos do ciclo de auditoria, desde o planejamento anual até a avaliação detalhada de riscos e testes de controles, bem como o acompanhamento de ações e relatórios do Comitê de Auditoria.

É possível definir uma estrutura de organização com qualquer número de níveis. Cada entidade auditável pode ser associada a um número de processos. Esta estrutura permite a análise e sintetização das avaliações de risco para mostrar quais auditorias ou análises dariam a cobertura de risco ideal. As auditorias podem abranger várias entidades e processos para atender a necessidade de auditorias temáticas ou funcionais de vários locais.

A figura a seguir apresenta as principais funcionalidades e objetivos do software Pentana:

Figura 10.6 – Software Pentana



10.2.4 Galileo

Galileo é um sistema de gestão de auditoria que pode ser adaptado às necessidades específicas de uma auditoria interna, investigações, conformidade ou outra necessidade orientada a projetos. Quando integrado com

outras plataformas de gestão de risco, ele fornece uma metodologia de auditoria baseada em risco, bem como modelos padrão de auditoria de risco. O sistema abrange o planejamento de auditoria estratégico e anual.

O sistema contempla também produção de relatórios de auditoria de forma automatizada. Outra funcionalidade abrange formulários de pesquisa pós-auditoria para obter feedback sobre o processo de auditoria, indicadores chave de desempenho e informações gerenciais para todas as atividades realizadas pelo departamento em questão.

O sistema oferece também opções de relatórios multidimensionais padrão e personalizados para garantir que as necessidades exatas do trabalho de auditoria sejam atendidas.

10.2.5 TeamMate

O software TeamMate fornece um conjunto completo de ferramentas para gerenciar o processo de auditoria. As principais funcionalidades do aplicativo incluem:

- × **planejamento de auditoria baseado em risco** – módulo denominado *TeamRisk*, auxilia os auditores na criação de avaliações de auditoria baseadas em risco que são compatíveis com padrões e normas atuais;
- × **documentação de auditoria** – módulo denominado *TeamEWP* (*Electronic Working Papers*) inclui funcionalidades de modo que todas as informações importantes, como etapas do programa, problemas, notas, assinaturas e históricos de edição estão contidas nas tabelas do banco de dados;
- × **agendamento de auditoria** – módulo denominado *TeamSchedule*, fornece aos usuários a capacidade de programar projetos e recursos de tal forma que há uma demonstração visual clara de atribuições de pessoal e rastreamento de projetos em um planejamento anual. Permite também que vários agendadores e equipes de recursos acessem as interfaces *Gantt* para exibir projetos e atribuições;
- × **relatório de tempo e despesas** – fornece ao software a capacidade de inserir tempo e despesas para projetos, eventos não-funcionais

como férias e tarefas administrativas. Permite acompanhar visualmente o andamento dos projetos e dos custos associados e gerar relatórios que resumem projetos, utilização de recursos e comparações com os orçamentos gerais dos departamentos.

10.3 Ferramentas específicas de auditoria de SI

Existem ferramentas de auditoria de sistemas de informação que são desenvolvidas especificamente para a execução de uma tarefa determinada. Tais ferramentas não apresentam foco generalista, com diversas funcionalidades, como as ferramentas abordadas nos tópicos anteriores. O foco principal é auxiliar o auditor em uma circunstância definida. O desenvolvimento deste software específico pode ser feito pela própria empresa de auditoria, caso possua mão de obra especializada, ou por terceiros contratados para esta finalidade.

A principal vantagem se deve ao fato de que, por ser desenvolvida para uma demanda específica, a eficiência da ferramenta é muito maior do que a de um software generalista. Existem certas áreas de atuação que demandam tarefas especializadas do segmento cuja auditoria será facilitada com o uso de um software específico da área.

Como desvantagem principal citamos o fato de que o desenvolvimento destas ferramentas costuma ser oneroso, visto que se tratam de softwares que atenderão somente a um cliente. A organização necessitará pesar o custo-benefício de desenvolver uma ferramenta própria para tarefas específicas de auditoria.

10.4 Ferramentas de uso geral para auditoria de SI

Nesta categoria enquadram-se todos os outros softwares que possuem funcionalidades comuns não só à área de auditoria, mas também com outras áreas de Tecnologia da Informação. Podemos citar como exemplo aplicativos que manipulam arquivos, efetuando sua ordenação, concatenação etc., bem como ferramentas de geração de relatórios automatizados.

Programas utilitários em geral não são desenvolvidos especificamente para a área de auditoria, portanto não apresentam recursos como verificação de gravação de trilhas de auditoria, por isto devem ser utilizados somente em caso de impossibilidade de uso de outras ferramentas específicas da área de auditoria, ou como complemento destas.

Síntese

Neste capítulo estudamos a importância do uso de ferramentas apropriadas para que o trabalho do auditor de sistemas de informação seja desenvolvido de forma eficiente. Estudamos as principais ferramentas generalistas utilizadas no mercado, como a ACL, e suas seis fases de desenvolvimento de um projeto de auditoria. Os conceitos de ferramentas generalistas, específicas e de uso geral orientam os auditores a procurar a melhor solução no desenvolvimento do trabalho de auditoria.

Atividades

1. Avalie a frase a seguir: “o software *Audit Command Language* faz parte da categoria de softwares especializados em auditoria, visto que possui diversas funcionalidades, podendo ler bases de dados de diversos formatos”.
 - a) Certo
 - b) Errado
2. Faça a devida correlação entre as fases de um projeto ACL.
 - ✗ Planejar o projeto
 - ✗ Adquirir os dados
 - ✗ Acessar os dados com o ACL
 - ✗ Verificar a integridade dos dados
 - ✗ Analisar os dados
 - ✗ Reportar os achados

- () Assegurar-se de que os dados não contenham elementos corrompidos.
 - () Identificar o objetivo em termos comerciais e técnicos.
 - () Preparar os resultados para apresentação formal.
 - () Obter acesso físico e lógico identificando a localização e o formato dos dados de origem necessários.
 - () Interrogar e manipular os dados para identificar exceções.
 - () Adicionar dados ao projeto como tabelas, que definem como a ACL lê os dados de origem.
3. O software IDEA permite auditoria baseada em gestão de risco, por meio de governança organizacional e alto desempenho operacional.
- a) Certo
 - b) Errado
4. As ferramentas específicas de auditoria de SI possuem a vantagem de serem desenvolvidas para uma demanda específica, por isso a eficiência da ferramenta é muito maior do que um software generalista, além de ter custo baixo de produção, visto que possui menos funcionalidades que necessitam ser desenvolvidas.
- a) Certo
 - b) Errado

Conclusão

Abordamos nesta obra um dos temas mais relevantes da atualidade para a área de Tecnologia da Informação e Comunicação. A preocupação com a Segurança da Informação não é mais exclusividade dos administradores de TI, pois todos os usuários finais precisam estar cientes do seu papel neste processo de proteção de um dos ativos mais valiosos de uma organização: a informação.

Apresentamos conceitos fundamentais, como os pilares da Segurança da Informação, formas de classificação e ciclo de vida da informação, bem como orientações aos gestores de como implementar uma política de Segurança da Informação que seja bem-sucedida em sua organização. Para tal, é imprescindível conhecer as principais normas e padrões adotados mundialmente relacionados à esta área, em especial as normas da família ISO 27000.

Dedicamos boa parte de um capítulo para o estudo das técnicas e formas de proteção contra a Engenharia Social, pois de nada adianta investimento maciço em tecnologia, se o elo mais fraco, o fator humano, não for considerado pelos administradores de TI.

Nesta obra, também detalhamos os principais conceitos, metodologias e técnicas de Auditoria de Sistemas de Informação. Uma organização tem sua credibilidade reforçada quando utiliza métodos adequados para Auditoria de Sistemas. Além de trazer estes principais métodos e técnicas, também apresentamos algumas das ferramentas mais utilizadas para este fim.

A você, aluno, esperamos que o estudo desta obra tenha sido proveitoso!

Gabarito

1. Conceitos e Princípios de Segurança da Informação

1. **Dados:** elementos fundamentais e brutos (matéria-prima da informação).

Informação: conjunto de dados, que possui um significado dentro de um contexto.

Conhecimento: quando um conjunto de informações constitui um saber.

A compreensão destes conceitos auxilia na compreensão geral do valor que a informação e o conhecimento possuem dentro de uma organização.

2. Confidencialidade, integridade, disponibilidade, autenticação, não-repúdio, legalidade, privacidade e auditoria.

Cada um destes conceitos deve ser plenamente conhecido pelo profissional de Tecnologia da Informação que preza pela Segurança da Informação em sua organização.

3. B. Uso

O uso é a etapa mais importante, pois saber exatamente como usar a informação leva a organização a gerar valor sobre esta.

4. B. Errado

Esta descrição corresponde ao nível de classificação “secreto”, um nível acima de “confidencial”.

2. Metodologias e Padrões de Segurança da Informação

1. Um sistema de gerenciamento de segurança da informação (SGSI) é um conjunto de políticas e procedimentos para gerenciar sistematicamente os dados sensíveis de uma organização. O objetivo de um SGSI é minimizar o risco e garantir a continuidade do negó-

cio pró-ativamente limitando o impacto de uma violação de segurança. A importância de sua implementação reside no fato de que ao estabelecer o SGSI, a organização pode determinar o nível de segurança necessário, fazer planos e distribuir seus ativos com base em sua própria avaliação de risco, além de contramedidas técnicas contra cada questão individual, garantindo assim a confidencialidade, integridade e disponibilidade de seus ativos de informação.

Entender o conceito de SGSI é fundamental para que o profissional de Tecnologia da Informação atente-se ao fato de que proteger a informação é proteger um dos ativos mais valiosos de uma empresa.

2. Embora uma organização possa implementar vários tipos de controles lógicos para garantia da segurança da informação, o acesso não autorizado a uma área sensível, como *datacenter*, por exemplo, pode causar um incidente de segurança grave. Caso um funcionário mal-intencionado com conhecimentos suficientes em atividade *hacker* possua acesso físico ao servidor corporativo de dados, a inserção de um dispositivo portátil de armazenamento contaminado para este fim poderá comprometer a segurança do equipamento e dos dados contidos neste.

Os tópicos da norma, embora possam parecer muito teóricos em uma primeira leitura, apresentam aplicação prática em vários aspectos, como é o caso do exemplo citado neste exercício.

3. Os cinco princípios do COBIT são:

- ✗ Atender as necessidades das partes interessadas;
- ✗ Cobrir a empresa de ponta a ponta;
- ✗ Aplicar um framework único e integrado;
- ✗ Permitir uma abordagem holística;
- ✗ Distinguir a governança da gestão;

Os princípios auxiliam a compreender como o COBIT é baseado em controles, servindo como referência a uma organização que deseja ter uma governança de TI mais controlada.

4. Os componentes básicos que compõem o ITL são o Núcleo e os Guias Complementares. No núcleo encontram-se as orientações sobre as melhores práticas aplicáveis e nos guias complementares existem orientações destinadas especificamente para setores, tipos de organização, modelos operacionais e arquiteturas de tecnologia.

Organizações que desejam implementar de gerenciamento de serviços de TI devem iniciar pelos componentes básicos, sendo que os guias complementares destinam-se a setores e tipos específicos de organizações.

3. Procedimentos e Boas Práticas de Segurança da Informação

1. O IPv6 apresenta melhorias significativas quanto comparado à sua versão IPv4, uma vez que tem implementações de segurança obrigatórias, não mais opcionais. Isso significa que as comunicações serão protegidas no nível mais baixo possível, via *IPsec*, onde cada pacote enviado terá de ser descriptografado para que possa ser interpretado.

O conhecimento das melhorias de segurança implementadas na versão 6 do protocolo IP são fundamentais para os administradores de rede, visto que tal versão será cada vez mais adotada em larga escala nas organizações.

2. Caso seja necessário que alguns recursos de rede, como um servidor web ou servidor FTP, esteja disponível para usuários externos, é preciso que esses recursos estejam em uma rede separada por trás do *firewall*, denominada DMZ (zona desmilitarizada). O *firewall* permite acesso limitado à DMZ, e como a DMZ só inclui os servidores públicos, um ataque externo só afeta os servidores e não afeta o restante da rede interna.

Administradores de ambientes de TI que necessitam disponibilizar serviços na web devem conhecer a fundo conceitos como DMZ, a fim de minimizar os impactos de um incidente de segurança em caso de violação.

3. Fator de conhecimento (senha) e fator de posse (smartphone).

Para serviços críticos de uma organização deve ser considerada a possibilidade de autenticação de fator múltiplo.

4. Os backups incrementais fazem apenas backup dos dados que foram alterados desde a última tarefa de backup. Já os backups diferenciais, por outro lado, farão backup de todos os dados que foram alterados desde o último backup completo.

Compreender a diferença entre os conceitos de backup auxiliará o administrador de TI a escolher qual a melhor estratégia, de acordo com a disponibilidade de espaço, bem como criticidade dos dados envolvidos.

4. Aspectos Tecnológicos da Segurança da Informação

1. Ambos são considerados *malwares*, porém a principal diferença é que o *worm* não necessita de uma intervenção humana para sua propagação, sendo esta realizada de maneira automatizada, enquanto os vírus necessitam de uma ação humana (por exemplo, a abertura de um aplicativo infectado).

Compreender a diferença de conceitos entre os diversos tipos de *malwares* auxilia na definição de estratégias de combate a estas infecções.

2. A concatenação de *strings* SQL sem validação de dados é uma das principais portas de entrada para ataques de injeção de código SQL malicioso, portanto seu uso deve ser evitado.

Existem melhores estratégias para a captura de dados que necessitam ser concatenados com cláusulas SQL, como por exemplo o uso de *Stored Procedures*.

3. A

A principal característica da criptografia simétrica é o uso de uma mesma chave para cifrar e decifrar a mensagem.

4. A. CERTO

A assinatura digital utiliza o conceito de par de chaves, onde a mensagem é cifrada utilizando-se da chave privada do emissor, e verificada pelo receptor utilizando a chave pública do emissor.

5. Aspectos Humanos da Segurança da Informação

1. Inicia-se com a **coleta**, que é a etapa de levantamento de informações sobre o alvo. Depois estabelece-se a **relação de confiança**, sendo a fase na qual o atacante passa a desenvolver um relacionamento com o alvo. A próxima é a **manipulação psicológica** do alvo para finalmente na etapa de **conclusão** efetuar-se uma saída discreta da situação.

Embora cada ataque de Engenharia Social seja único, compreender o ciclo auxilia em uma estratégia de defesa contra tais ataques.

2. A

Os ataques de Engenharia Social via de regra baseiam-se no estabelecimento de uma relação de confiança com a vítima.

3. *Phishing* é a prática de usar e-mails de spam para induzir um indivíduo a revelar informações privadas que podem ser usadas para roubo de identidade. A melhor maneira de se proteger contra fraudes de *phishing* é nunca clicar em um link que pede que se visite um site para qualquer finalidade. O acesso deve ser feito diretamente pelo navegador do usuário.

Embora exista muita informação disponível na internet sobre como evitar os ataques de *phishing*, muitos usuários leigos ainda são afetados por este tipo de golpe.

4. Este profissional tem habilidades comprovadas para realizar testes de invasão em sistemas computacionais, utilizando-se de varreduras e conhecimentos *hackers*, explorando vulnerabilidades a fim de redigir um relatório técnico com recomendações de segurança.

Atualmente cada vez mais empresas têm contratado os serviços dos profissionais que realizam testes de invasão, a fim de identificar quais são as principais vulnerabilidades em seus ambientes computacionais passíveis de exploração por parte de invasores.

6. Gerenciamento de Riscos em Segurança da Informação

1. Se a análise de riscos é realizada na fase de especificação da necessidade e escopo do sistema, é possível incluir os riscos identificados no desenvolvimento dos requisitos do sistema, melhorando assim sua segurança.

Incluir requisitos de segurança nesta fase significa diminuir custos de implantação de processos e procedimentos de segurança posteriores, evitando assim que vulnerabilidades possam ser exploradas futuramente.

2. As ameaças são possibilidades de exploração de vulnerabilidades. A vulnerabilidade é uma fraqueza do sistema que pode ser explorada.

A ameaça somente representa um risco quando existe uma vulnerabilidade passível de ser explorada.

3. A. Sim

O risco é aceitável pois dificilmente uma vulnerabilidade será explorada se o custo do ataque não representar um retorno vantajoso ao atacante.

4. Iniciação, desenvolvimento ou aquisição, implementação, operação ou manutenção e eliminação.

O gerenciamento de riscos é um processo que pode ser realizado de forma iterativa para cada fase principal do CVDS, sendo que sua implementação auxilia na mitigação de impactos negativos em caso de incidentes de segurança envolvendo os sistemas.

7. Fundamentos em Auditoria de Sistemas de Informação

1. A relação de agência é um contrato sob o qual uma ou mais pessoas (os principais) contratam outras pessoas (o agente) para desempenhar algum serviço que envolva delegação de alguma decisão ao agente. Portanto, quando acionistas investem em uma empresa e existem gerentes responsáveis por administrar a empresa, o que vemos é uma relação de agência. Os acionistas são os principais e os gerentes são os agentes. Podemos visualizar a mesma relação em empresas públicas. Quando um servidor público administra um órgão público, ele está atuando como o agente e, neste caso, a sociedade é o principal.

Quando se contrata um auditor, busca-se a opinião de um terceiro, que deve ser independente e objetiva. O auditor deve verificar se as decisões dos agentes respeitam os interesses do principal. Exemplificando, o auditor deve verificar se os gestores públicos de um hospital federal, como agentes, estão investindo o dinheiro repassado ao hospital para servir bem a sociedade. Estes têm o papel de principal, o interesse da sociedade é ter um bom serviço público. Do mesmo modo, os acionistas de um hospital particular contratam uma auditoria para verificar se os diretores do hospital, os quais possuem o papel de agentes, estão tomando decisões para alcançar os objetivos dos acionistas, que têm o papel de principais. Na empresa privada usualmente este objetivo é o lucro.

Assim, a teoria da agência demonstra o conflito de interesses existentes entre o papel do principal e o papel do agente, o que auxilia a compreender o papel do auditor.

2. Devido ao crescimento das corporações e ao volume das transações realizadas, tornou-se economicamente inviável auditar a totalidade das transações. A amostragem é uma técnica para reduzir o universo de análise. Entretanto, com a redução do universo de análise, cria-se a probabilidade de que a auditoria não encontre fatos e registros importantes caso a informação com o registro da evidência esteja em um ativo não-auditado. Portanto, o auditor

deve escolher a amostra a ser auditada com técnicas estatísticas e de análise de riscos.

Afirmar que uma auditoria por amostras não diminui a eficácia da auditoria seria imprudente. No entanto, a escolha das amostras deve ser executada para diminuir o denominado risco da auditoria. Portanto, procura-se escolher as amostras com mais probabilidade de conter achados de auditoria e evidências de inconformidades. Para isso serão utilizadas técnicas estatísticas e de análise de risco.

3. Controles internos são planos organizacionais e coordenação de um conjunto de métodos e medidas adotados em uma empresa, a fim de salvaguardar o ativo, verificar a exatidão e veracidade de registros contábeis, promover a efetividade de sistemas de informação contábil e eficiência operacional, assim como fomentar uma grande adesão às políticas da organização. Portanto, um controle interno eficiente diminui a possibilidade de desvios nos processos existentes na empresa.

Controles internos fazem parte de uma administração eficiente. Assim, os controles internos também são alvos da auditoria em uma empresa.

Além disso, atualmente, devido ao tamanho das organizações e à quantidade de transações existentes, é impossível, economicamente, realizar a auditoria extensiva de todas as transações de uma empresa. Os auditores demorariam muito tempo e o valor da auditoria seria extremamente alto. Deste modo, os auditores usualmente utilizam amostras. A escolha das amostras é realizada utilizando uma abordagem baseada na análise de riscos. De maneira simples, bons controles internos diminuem a probabilidade de problemas de auditoria. Portanto, os controles internos também auxiliam na escolha das amostras que têm mais riscos de possuírem problemas. Áreas com controles internos deficientes deverão ser auditadas com maior rigor.

4. O risco da auditoria é uma junção de três riscos: risco inerente, risco de controle e risco de detecção.

- ✗ O **risco inherente** pode ser definido como o risco do próprio negócio, influenciado pela natureza sua natureza. Portanto, áreas diferentes de atuação possuem riscos diferentes. Por exemplo, um software de controle de voo tem um risco muito maior – pois o impacto de qualquer problema é muito grande – quando comparados com o risco de um sistema de controle de pedágio.
- ✗ O **risco de controle** está relacionado à existência de erros materiais, que não sejam detectados ou previstos pelos controles internos da organização. Devido à própria natureza e custo dos controles internos, é improvável que um controle interno evite totalmente o risco de uma inconformidade.
- ✗ O **risco de detecção** é o risco existente dos procedimentos realizados pelo auditor não detectarem uma deficiência com materialidade nos sistemas de informação.

O auditor deve trabalhar para diminuir o risco da auditoria, garantindo a confiabilidade do trabalho realizado.

8. Metodologia de Auditoria de Sistemas de Informação

1. A IPPF descreve na norma de desempenho 2000 que o auditor chefe executivo é responsável por gerenciar de forma eficaz a atividade de auditoria interna para assegurar que ela adicione valor à organização. É também seu dever assegurar que os recursos são apropriados, suficientes e efetivamente utilizados para realizar o plano de auditoria aprovado. Deve deter um conhecimento sobre o negócio e os controles internos existentes na empresa, mas não é obrigado a conhecer todas as tecnologias existentes dentro da empresa.

É também dever do auditor chefe executivo o plano de auditoria. Neste plano deverão estar especificados os objetivos específicos, escopo e critérios da auditoria, assegurando que a auditoria adicione valor para a organização. O plano deverá especificar o que será auditado, por que e como será auditado.

O auditor chefe executivo funciona como uma interface entre o comitê de auditoria, a gerência e os auditores de sistemas de informação, garantindo que a auditoria seja realizada de maneira objetiva e independente.

2. Letra C.

Alternativa A: Falsa

A definição das normas de atributos são normas que endereçam as características das organizações e dos indivíduos que executam auditoria interna. Portanto, não se restringem às características dos profissionais, mas também das organizações.

Alternativa B: Falsa

O código de ética do IIA tem quatro princípios: integridade, objetividade, confidencialidade e competência.

Alternativa C: Verdadeira

A definição da auditora interna está presente no capítulo 7 deste livro.

- ✗ A auditoria interna é uma atividade independente, de garantia e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Assiste à organização na consecução dos seus objetivos, por meio de uma abordagem sistemática e disciplinada, para a avaliação e melhoria da eficácia dos processos de gestão de risco, controle e governação (IIA, 2013).

Esta definição dá base para encontrarmos qual a resposta correta para a questão.

Alternativa D: Falsa

Para compreender qual a falácia nesta afirmação, podemos remeter à teoria da agência. Existem dois papéis principais: o principal e o agente. O auditor entra como um terceiro papel, garantindo que o agente está trabalhando no melhor interesse do principal. Portanto, existem três papéis básicos em uma auditoria:

1. a pessoa ou o grupo diretamente envolvido com a entidade, operação, função, processo, sistema, ou qualquer que seja o ativo auditado, desempenha o papel do agente.
2. a pessoa ou o grupo que efetua a avaliação é o auditor interno.
3. a pessoa ou o grupo que utiliza a avaliação é o principal ou usuário.

Alternativa E: Falsa

Existem dois principais tipos de normas: as normas de atributos e as de desempenho. Adicionalmente, existem as normas de implantação, com o objetivo de especificar detalhes dos outros dois tipos de normas e prover os requisitos aplicáveis às atividades de avaliação ou consultoria. Portanto, não existem normas de responsabilização

3. Como já definido, metodologia significa o estudo dos métodos, ou seja, a metodologia é a explicação, detalhada, rigorosa e precisa de toda ação desenvolvida no método de trabalho, sendo o método o caminho necessário para se chegar a um fim.

Desta forma, a metodologia garante que os métodos possíveis para a realização da metodologia foram estudados e que o método escolhido conseguirá atingir os resultados necessários. As mudanças no funcionamento, tamanho e objetivo das organizações tiveram alta influência nos métodos e técnicas utilizadas para a realização de uma auditoria. O crescimento das empresas incorreu na utilização da amostragem nas auditorias. Auditorias governamentais, realizadas por EFS, têm métodos diferentes que auditorias de empresas privadas. Auditorias internas e externas utilizam métodos diferentes.

A escolha correta do método, portanto, afeta a eficiência e eficácia da auditoria. A eficiência garantindo a melhor utilização dos recursos disponíveis, e a eficácia diminuindo os riscos da auditoria, apresentando as técnicas e papéis necessários para a execução da auditoria com a independência e objetividade necessária. Deste modo, podemos dizer que a metodologia altera, também, a credibilidade da auditoria.

4. Cada um destes tipos de auditoria tem os seus objetivos e metodologias. A auditoria externa diferencia-se principalmente por ser

realizada por uma organização independente e externa de auditoria. A auditoria externa busca o maior grau possível de independência com a empresa auditada. A auditoria interna, por sua vez, diz respeito ao vínculo mantido entre o auditor e a entidade auditada. Em uma auditoria interna a unidade da auditoria integra a estrutura da organização.

A auditoria interna diferencia-se, no seu objetivo, da auditoria externa, pois tem como foco auxiliar os gestores a alcançar os objetivos da empresa, enquanto a auditoria externa tem por objetivo prestar informações ao principal. Portanto, uma auditoria externa usualmente busca um terceiro confiável com credibilidade entre todos os interessados no resultado da auditoria. Consequentemente, para atingir o objetivo deste tipo de auditoria é necessário ter credibilidade perante a sociedade no quesito auditado. A empresa de auditoria externa contratada deve ser um terceiro confiável. Esta é uma grande diferença da auditoria interna, a qual é realizada por empregados da própria empresa. Apesar de ainda ser observado um alto grau de independência para auditores, este tipo de auditoria não gozaria de fé perante aos muitos interessados externos à empresa, pois defenderiam os interesses da própria empresa. No entanto, a auditoria interna tem um papel muito importante para as organizações, pois seu objetivo é, como já escrito, buscar auxiliar a organização a alcançar os seus objetivos e metas, além de poder funcionar como preparação para uma auditoria externa que usualmente tem um custo muito mais alto que uma auditoria interna.

9. Técnicas e Melhores Práticas de Auditoria de Sistemas de Informação

1. B. ERRADO

A técnica caracteriza-se por testar as funcionalidades de entrada de dados em um sistema, e não saída.

2. As entrevistas diretivas destinam-se a obter informações específicas sobre fatos verificáveis (por exemplo: procedimento para pagamento de fatura de compra), enquanto a entrevista não-diretiva

tem como objetivo obter compreensão geral e construir uma relação de confiança com o auditado.

Em muitos casos, durante a fase de entrevistas, será necessário utilizar-se dos dois métodos, iniciando-se com uma entrevista diretiva para obtenção de informações essenciais, e finalizando com a abordagem não-diretiva, a fim de que o entrevistado amplie a discussão.

3. A. Preparação

As normas podem variar de acordo com o tipo de auditoria, políticas da organização e certificações profissionais do auditor.

4. A. CERTO

Dentre os seis objetivos principais este destaca-se em especial, no contexto da segurança da informação.

10. Ferramentas de Auditoria de Sistemas de Informação

1. B. ERRADO

O software especializado é desenvolvido para a execução de uma tarefa específica, diferentemente do software generalista, capaz de realizar tarefas diversificadas.

2. 4-1-6-2-5-3

O projeto de auditoria desenvolvido com o software ACL, via de regra, respeita todas as seis etapas descritas.

3. B. ERRADO

Estas são características presentes no software Pentana.

4. B. ERRADO

O custo de desenvolvimento de uma ferramenta específica costuma ser oneroso, visto que trata-se de um software que atenderá somente a um cliente.

Referências

ABNT. 2011. **ABNT NBR ISO 19011**. Diretrizes para auditoria de sistemas de gestão. Rio de Janeiro: ABNT, 2012.

ARIMA, C. H. **Auditoria de Sistemas de Informação**. Revista de Administração, v. 28, 1993.

AUDIT COMMAND LANGUAGE. **ACL**. Disponível em: <<http://www.acl.com>>. Acesso em: 20 jan. 2016.

BBC. **Backup** – technical implementation. Disponível em: <<http://www.bbc.co.uk/education/guides/zws3gk7/revision/4>>. Acesso em: 20 nov. 2016.

BOECKH, A. **The public economy of Athens**. Berlin: Baxter, 1817. Volume 1.

BSI. **Information security audit** – a guideline for IS audits based on IT-Grundschutz. Bonn: German Federal Office for Information Security, 2008.

CASTANHEIRA, N. M. C. **Auditoria interna baseada no risco**: estudo do caso português. Dissertação (Mestrado em Contabilidade e Auditoria). Universidade do Minho, Braga, 2007.

CERT.br. **Glossário**. Disponível em: <<http://cartilha.cert.br/glossario>>. Acesso em: 15 dez. 2016.

_____. **Incidentes reportados ao CERT.br**. Janeiro a Dezembro de 2015. Disponível em: <<http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque-acumulado.html>>. Acesso em: 20 nov. 2016.

_____. **Total de incidentes reportados ao CERT.br por ano**. 2016. Disponível em: <<http://www.cert.br/stats/incidentes>>. Acesso em: 20 nov. 2016.

CRISTO, C. A. de; SILVA, E. L. da. 2005. A função ética e a responsabilidade social do auditor na análise das demonstrações contábeis. **Contábeis**. o portal da profissão contábil, 2005. Disponível em: <<http://www.contabeis.com.br/artigos/34/a-funcao-etica-e-a-responsabilidade-social-do-auditor-na-analise-das-demonstracoes-contabeis/>>. Acesso em: 6 mar. 2017.

FAGUNDES, L. L. **Introdução à gestão da Segurança da Informação**. 2012. Disponível em: <<http://professor.unisinos.br/llemes/Aula01/Aula01.pdf>>. Acesso em: 20 nov. 2016.

- FERREIRA, F. N. F.; ARAÚJO, M. T. **Políticas de Segurança da Informação** – guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.
- HALL, J. A. **Accounting information systems**. 7. ed. Manson: South Western, 2011.
- HORWATH SOFTWARE. **Galileo**. Disponível em: <www.horwathsoftware.com/>. Acesso em: 20 jan. 2016.
- IBRACON. **Auditória**: registros de uma profissão. Ipsilon, 2007.
- ICAI. 2010. **Information Systems Control and Audit**. New Delhi: ICAI, 2010.
- IDEA. **Data Analysis**. Disponível em: <<https://www.casewareanalytics.com/products/idea-data-analysis>>. Acesso em: 20 jan. 2016.
- IDEAGEN PLC. **Pentana**. Disponível em: <<https://www.ideagen.com/products/pentana/>>. Acesso em: 20 jan. 2016.
- IIA. **Internal audit manual**. Florida: IIA, 1998.
- _____. 2013. Definition of Internal Auditing. **Institute of Internal Auditors**, 2013. Disponível em: <<https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx>>. Acesso em: 6 mar. 2017.
- IMONIANA, J. O. **Auditória de Sistemas de Informação**. 3. ed. São Paulo: Atlas, 2016.
- ISACA. 2007. **IT Assurance Guide: Using COBIT**. s.l.: IT Governance Institute, 2007. ISBN 1-933284-74-9.
- _____. **COBIT 5**. Disponível em: <<http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx>>. Acesso em: 20 nov. 2016.
- _____. **Information Systems Auditing: Tools and Techniques**. Disponível em: <<https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/information-systems-auditing-tools-and-techniques.aspx>>. Acesso em: 5 jan. 2017.

_____. **IT standards, guidelines, tools and techniques for audit and assurance and control professionals.** 2010. Disponível em: <<https://www.isaca.org/knowledge-center/standards/documents/it-audit-assurance-guidance-1march2010.pdf>>. Acesso em: 11 mar. 2017.

ISO. **ISO Standards.** Disponível em: <<http://www.iso.org>>. Acesso em: 20 nov. 2016.

ITI. **Sobre a ICP-Brasil.** Disponível em: <<http://www.iti.gov.br/acesso-a-informacao/96-perguntas-frequentes/1744-sobre-a-icp-brasil>>. Acesso em: 10 dez. 2016.

ITIL. **ITIL V3 Edition.** 2011. Disponível em: <<http://blog.itil.org/2014/11/elearning/itil-v3-edition-2011/>>. Acesso em: 20 nov. 2016.

JENSEN, M. C.; MECKLING, W. H. Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. **Journal of Financial Economics**, v. 3, 1976.

LYRA, M. R. **Segurança e Auditoria em Sistemas de Informação.** Rio de Janeiro: Ciência Moderna, 2008.

MACEDO, D. **Conceito de DMZ.** Disponível em: <<http://www.diegomacedo.com.br/conceito-de-dmz/>>. Acesso em: 20 nov. 2016.

MENDES, A. R. V. dos S. **Identificação dos fatores influenciadores para a escolha de uma profissão:** estudo de caso do Revisor Oficial de Contas nos distritos de Santarém e Leiria. 2013.

MICHAELIS. **Michaelis Dicionário Brasileiro da Língua Portuguesa.** s. l.: Melhoramentos, 2015.

NIST. SP800-30. **Risk management guide for information technology systems.** 2002. Disponível em: <<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>>. Acesso em: 20 dez. 2016.

OLIVEIRA, R. R. **Criptografia simétrica e assimétrica:** os principais algoritmos de cifragem. Disponível em: <<http://www.ronielton.eti.br/publicacoes/artigorevistassegurancadigital2012.pdf>>. Acesso em: 10 dez. 2016.

PINHO, R. C. de S. **Fundamento de Auditoria.** São Paulo: Atlas, 2007.

- PORTER, M. E. **Competição** On Competition: estratégias competitivas essenciais. s. l.: Elsevier, 1999.
- REHAGE, K.; HUNT, S.; NIKITIN, F. 2008. **Developing the IT Audit Plan**. s.l.: The Institute of Internal Auditors, 2008.
- RICHARDS, D. A.; OLIPHANT, A. S.; GRAND, C. H. L. 2005. **Information Technology Controls**. Flórida: IIA, 2005.
- SAFECODE. **Fundamental Practices for Secure Software Development**. 2. ed. Disponível em: <https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf>. Acesso em: 10 dez. 2016.
- SEGINFO. **As 8 certificações mais requisitadas na área de segurança de TI**. Disponível em: <<https://seginfo.com.br/2015/07/28/as-8-certificacoes-mais-requisitadas-na-area-de-seguranca-de-ti-2/>>. Acesso em: 15 dez. 2016.
- TCPE. **Política de uso aceitável dos recursos de tecnologia da informação do tribunal de contas do estado de Pernambuco**. Disponível em: <<http://www.tce.pe.gov.br/internet/docs/resolucoes/14res0017.pdf>>. Acesso em: 20 nov. 2016.
- TCU. 2011. **Auditoria governamental**, 2011.
- _____. **Auditoria realizada pela 4ª. SECEX sobre concessão de benefícios previdencários no Instituto Nacional do Seguro Social – INSS**. s.l.: TCU, 2001.
- _____. **Governança de TI**. Disponível em: <<http://portal.tcu.gov.br/comunidades/governanca-de-ti/entendendo-a-governanca-de-ti/>>. Acesso em: 20 nov. 2016.
- _____. **Manual de auditoria operacional**. Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog), 2010.
- TEAMMATE SOLUTIONS. **TeamMate**. Disponível em: <<https://www.teammatesolutions.com>>. Acesso em: 20 jan. 2016.
- TJPE. Termo de Responsabilidade – **Política de Segurança da Informação**. Disponível em: <https://www.tjpe.jus.br/intranet/drh/Termo_Responsabilidade_Politica_Seguranc.doc>. Acesso em: 20 nov. 2016.

Este livro apresenta assuntos atuais e relevantes, que não podem ser negligenciados pelas organizações como um todo. A Segurança da Informação trata de assuntos muito presentes em nosso cotidiano, seja em um ambiente corporativo ou pessoal. Já a Auditoria de Sistemas tem importância estratégica para corporações, visto que os sistemas possuem informações vitais para elas.

Abordaremos conceitos fundamentais de segurança da informação, como a forma de classificar a informação, seu ciclo de vida e políticas que devem ser implementadas. No capítulo dedicado às normas da família NBR ISO/IEC 27000, além de COBIT e ITIL, conheceremos a fundo os regulamentos e padrões que são adotados mundialmente. Aspectos tecnológicos fundamentais, bem como aspectos humanos para garantia da segurança da informação também serão detalhados nesta obra.

Os quatro últimos capítulos são dedicados à Auditoria de Sistemas de Informação, nos quais detalharemos fundamentos, metodologia, técnicas e melhores práticas, bem como exemplos de ferramentas que auxiliam neste processo.

ISBN 978-85-60531-78-3



9 788560 531783