Marcus Leal Dantas

SEGURANÇA DA INFORMAÇÃO

Uma Abordagem Focada em Gestão de Riscos

Auditor fiscal e Oficial da reserva da Polícia Militar de Pernambuco, possui trabalhos publicados e realizados nas áreas de segurança pública, privada, portuária, da informação e de gestão de riscos. É contador, graduado pela UFPE, e pós-graduado em planejamento e gestão organizacional pela FCAPE, e em Direito Tributário pela UFPE. É Auditor Líder em Sistemas de Gestão de Segurança da Informação ISO 27001:2005.

E-mail: marcusdantas@uol.com.br

Marcus Leal Dantas

SEGURANÇA DA INFORMAÇÃO: UMA ABORDAGEM FOCADA EM GESTÃO DE RISCOS

Livro Rápido
Olinda – PE
2011

Impresso no Brasil
Printed in Brazil

Editor
Tarcísio Pereira

Diagramação
Laís Mira

Capa
Braullio Andrew

Revisão
Professora Margarida Michel

Dados Internacionais de Catalogação na Publicação (CIP)
Ficha catalográfica

Dantas, Marcus Leal
D192s Segurança da informação: uma abordagem focada em gestão de riscos. / Marcus Leal Dantas. – Olinda: Livro Rápido, 2011.

152 p.

Bibliografia. p. 147 – 150 (bibliografia localizada)
ISBN 978-85-406-0047-8

1. Segurança da informação. 2. Informação – vulnerabilidades e ameaças. 3. Negócios corporativos. 4. Tecnologia da Informação. I. Título.

004.73:658 CDU (1997)
Fabiana Belo - CRB-4/1463

Livro Rápido – Elógica
Rua Dr. João Tavares de Moura, 57/99 Peixinhos
Olinda – PE CEP: 53230-290
Fone: (81) 2121.5300 Fax: (81) 2121.5333
www.livrorapido.com

SUMÁRIO

INTRODUÇÃO

As transmissões ao vivo dos ataques terroristas de 11 de setembro de 2001 às torres gêmeas do World Trade Center e ao Pentágono mostraram o povo em pânico pelas ruas, pessoas se jogando do alto das torres, o céu encoberto por uma poeira cinzenta, centenas de milhares de pedaços de papel e um grande volume de destroços. Como consequências, ocorreram milhares de mortes, o colapso dos serviços de transporte e comunicações, a destruição de muitas empresas, um dano irreparável e um enorme abalo na sensação de segurança do povo de um país tido como o mais seguro do mundo. Essas imagens assustadoras dificilmente deixarão as nossas mentes.

Em dezembro de 2004, um evento da natureza causou um grande estrago na Indonésia. As ondas gigantes, conhecidas como *tsunami*, não só acabaram com a alegria das festividades do ano vindouro, como destruíram povoados inteiros e levaram junto com elas centenas de milhares de vítimas, e todos pegos de surpresa. As imagens dessa catástrofe natural também serão difíceis de ser esquecidas.

Em fevereiro de 2008, uma das maiores empresas petrolíferas do mundo teve computadores portáteis furtados com informações estratégicas de uma reserva gigante, descoberta no ano anterior, estimada em torno de 8 bilhões de barris de petróleo, sendo considerada uma das maiores descobertas de petróleo dos últimos anos. As notícias sobre esse evento ocuparam as principais manchetes na mídia mundial, além de exporem a fragilidade da segurança da informação em uma empresa multinacional, o que provocou a apreensão nos seus acionistas.

Esses acontecimentos refletem o quanto é complexa a questão da segurança. Se, de um lado, os ataques terroristas de 11/09 mostraram os efeitos dos riscos de uma ação intencional que abalou fortemente o sistema de segurança da nação mais poderosa do mundo, por outro lado, as *tsunamis* deixaram claras as consequências dos riscos dos eventos da natureza, como também as falhas nos cuidados com o transporte de equipamentos com informações estratégicas sobre importante descoberta de petróleo.

Esses exemplos levantam uma questão peculiar: a proteção das informações. Em ambos os acontecimentos (ataques terroristas e *tsunami*),

muitas informações foram destruídas e com elas muitos negócios. As empresas que foram atingidas por esses fatos puderam continuar com suas atividades de negócios? As empresas que retornaram às suas atividades possuíam um plano de recuperação de desastres? Quantas pessoas morreram em consequência de equipamentos e sistemas que deixaram de funcionar?

É um fato que a evolução da tecnologia mudou a forma dos negócios. Hoje, a nova estrutura dos negócios corporativos é a tecnologia da informação, o seu sistema nervoso é a informação, e o seu ambiente, alcança, também, o ciberespaço. O mundo virtual e a sua capacidade de processamento tornaram a vida melhor ao facilitarem muitas coisas, e trouxeram consigo não só benefícios mas também ameaças à segurança da informação.

Como foi visto, muitas empresas que estavam no WTC e nos locais atingidos pelas ondas gigantes perderam todos os seus bancos de dados e informações preciosas que jamais serão recuperadas. E esse fato levanta uma reflexão sobre a forma de proteção da informação.

Nesse cenário moderno, a segurança da informação passa a ocupar um *status* de destaque, cuja importância não está apenas nas ferramentas para a detecção de invasão e proteção antivírus, mas num arcabouço de medidas voltadas para a prevenção, detecção, resposta, recuperação e continuidade.

Para interromper um negócio, não se faz necessário um atentado terrorista ou um evento da natureza da proporção de um *tsunami*. Para que isso aconteça, basta uma simples ação desatenciosa de um funcionário ao desabilitar o sistema de proteção de invasão e provocar um ataque de invasão ou negação de serviço, indisponibilizando os sistemas por algum período, ou ao negligenciar em não verificar periodicamente os equipamentos do sistema de detecção de incêndio, prejudicando o tempo de resposta ao fogo, levando à propagação de um incêndio na área do CPD, destruindo todos os sistemas de informação da empresa.

Imagine-se o impacto nas pessoas que lidam com a modernização dos serviços bancários. Para verificar esse choque, basta nos dirigirmos a um terminal de autoatendimento e observarmos a dificuldade das pessoas nos simples atos de utilizar um cartão magnético e digitar uma senha.

Procedimentos fáceis. Tão fáceis que se tornam vulneráveis à clonagem e ao roubo de identidade.

E no serviço público não é diferente. Quantos servidores não conseguem desempenhar suas atividades sem a utilização da tecnologia da informação, e quantos não sabem utilizá-la. Quantos beneficiários dos serviços de previdência social se defrontam com essa tecnologia, ficam assustados e não acreditam na evolução, retroagindo à idade da pedra, em que só acreditam naquilo que veem e podem apalpar.

E nas empresas, onde o sucesso dos negócios depende cada vez mais da competitividade, a busca frenética por informações para a tão almejada vantagem competitiva é a grande responsável pelos cuidados com a informação. É nesse cenário que surge um funcionário que, agindo intencionalmente ou não, vaza informações e comete outras ações que comprometem a segurança da informação e o sucesso dos negócios corporativos.

Esses fatos ocorrem diariamente em todo o mundo, nas diversas camadas sociais e nos mais variados tipos de negócios, sejam eles públicos ou privados. Isso não é privilégio de sociedades modernas ou de empresas desprotegidas, é fruto do desenvolvimento. É resultado, em parte, do choque tecnológico que demonstra a tamanha velocidade frente a uma modernização dos processos de trabalho e de negócios, e de um conjunto de outros fatores que contribuem para criar o melhor ambiente para a concretização das ameaças às informações, como, por exemplo: fraudes financeiras, ataques de vírus, invasão de sistemas, roubo de identidade, etc.

Estar 100% seguro é uma meta a ser perseguida. Um desafio. Se tratar da segurança pessoal já é difícil, imagine-se tratar da segurança da informação, em que a evolução tecnológica é cada dia mais veloz e não alcança toda uma sociedade em todos os seus níveis.

Nesse contexto, objetivando proporcionar uma visão abrangente e uma abordagem proativa para a proteção da informação dentro da complexa modernização da sociedade, é que escrevemos este livro.

Foram duas versões, uma completamente diferente da outra, uma viagem pelas entrelinhas do gerenciamento de riscos e da segurança da informação. A primeira, concluída em 2008, e a segunda, em 2009.

O livro traz uma abordagem focada no gerenciamento de riscos da informação, apresentando aspectos importantes, que vão desde a concepção do que seja a informação, suas vulnerabilidades, ameaças e riscos, até a forma de gerenciar esses riscos.

O público-alvo é a comunidade da informação, especialistas em segurança, estudantes, pesquisadores e leigos de uma forma geral.

Com a nossa pesquisa, esperamos contribuir com a literatura sobre o assunto, de modo a poder difundir cada vez mais os conceitos modernos de segurança da informação, bem como melhorar o senso crítico dos leitores a respeito dessa tão polêmica e importante questão que é a **segurança da informação**.

Ao leitor, uma leitura instigante.

O autor

1. COMPREENDENDO A INFORMAÇÃO, SUAS VULNERABILIDADES E AMEAÇAS

O mundo moderno tem dedicado especial atenção à informação, devido à sua importância para a manutenção dos negócios e a realização de novos empreendimentos entre pessoas, empresas, povos, nações e blocos econômicos.

A boa informação abre verdadeiras oportunidades para quem a possui, o que torna o cenário dos negócios mais dinâmico e acirrado em busca de novos mercados, acordos internacionais, poder e qualidade, dentre outros, o que gera a competitividade e transforma a informação no principal elemento motriz desse ambiente altamente competitivo, que requer, assim, proteção especial.

Em contrapartida, a ausência da informação ou a informação de má qualidade constitui uma grande ameaça, podendo levar empresas à extinção. Tudo isso atribui à informação um importante valor, transformando-a num ativo essencial aos negócios de uma organização, necessitando ser protegida. Para a sua devida proteção, é preciso compreendê-la.

No ambiente da informação, permeiam alguns conceitos, nos quais encontramos definições específicas para **dados, informação, conhecimento e inteligência**. Esses conceitos alcançam áreas específicas, como, por exemplo, a militar, cuja atividade de inteligência está voltada para defesa do Estado, e a empresarial, que direciona essa atividade para os negócios.

Os **dados** compreendem a classe mais baixa da informação. A **informação** propriamente dita são os dados que passam por algum tipo de processamento para serem utilizados de uma forma inteligível. O **conhecimento** é a informação cuja relevância, confiabilidade e importância foram avaliadas, e é obtido pela interpretação e integração de vários dados e informações para iniciar a construção de uma situação. A **inteligência** é a informação com oportunidade, ou seja, é a parte do conhecimento que habilita a tomada das melhores decisões (Cardoso Júnior, 2005).

Nesse sentido, por exemplo, ao se pretender atingir um grande número de clientes para uma campanha promocional, a informação básica (dados) seriam os dados de cada cliente (idade, forma de aquisição: à vista ou

a crédito, preferência de itens de bens de consumo ou serviço), e uma variedade de dados que, após serem processados, formariam o perfil de poder de compra dos clientes (informação) para, junto a outras informações de preços de produtos de concorrentes, custos de aquisição, potencialidade do mercado, etc., poder criar uma situação (conhecimento) para a utilização mais vantajosa da campanha promocional, alavancando a competitividade e alcançando o sucesso esperado (inteligência).

Outro ponto importante é compreender um sistema de informações. Ralph (2002) conceitua **sistema de informação** como um conjunto de elementos ou componentes inter-relacionados, que coletam (entrada), manipulam (processamento) e disseminam (saída) os dados e a informação e fornecem um mecanismo de *feedback* para atender um objetivo.

COMPONENTES DE UM SISTEMA DE INFORMAÇÃO

Fonte: Ralph (2002).

Um sistema de informações bem estruturado é indispensável para a utilização da informação com oportunidade, isto é, para a tomada de decisões que ofereça competitividade.

Essa competitividade é alcançada pela **inteligência competitiva**, processo pelo qual as informações de múltiplas fontes são coletadas, interpretadas e comunicadas a quem precisa delas para decidir (Cardoso, 2005).

Observe-se que um é meio para a outra, pois, para se obter a inteligência competitiva, faz-se necessário possuir um excelente sistema de informações.

Mesmo reconhecendo essas diferenças, para a segurança da informação, todas essas segregações serão incluídas num único contexto: o da informação. Dados, informação, conhecimento ou inteligência, para a **segurança da informação**, tudo deve ser visto como informação.

1.1 Características da informação

Para ser utilizada, a informação necessita garantir três características fundamentais: a integridade, a disponibilidade e a confidencialidade, características que devem ser preservadas, pois são tidas como princípios da segurança da informação.

A **segurança da informação** é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio (NBR ISO/IEC 27002:2005).

Por definição, essa norma define a segurança da informação como:

"Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas."

Ao se falar em segurança da informação, deve-se levar em consideração essas qualidades da informação, pois toda ação que venha a comprometer qualquer uma dessas qualidades estará atentando contra a sua segurança.

Integridade

A integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento (NBR ISO/IEC 27002:2005).

Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente.

Ocorre a quebra da integridade quando a informação é corrompida, falsificada, roubada ou destruída. Garantir a integridade é manter a informação na sua condição original.

Acesso indevido em Empresa de publicidade[1,2]

Em recente caso, uma organização de publicidade australiana teve quebrado o controle de acesso ao sistema de folha de pagamento. O sistema foi invadido e explorado com o conhecimento do nível de vulnerabilidade do sistema. A companhia não tinha habilitado o registro para a rede de trabalho, base de dados ou nível de operação de sistemas que fornecesse aos investigadores uma trilha de investigação. Controles e cultura pobres de segurança tornaram fácil para o invasor esconder a sua presença.

Investigadores descobriram que ambos, o sistema de folha de pagamento e os administradores de terminais, tinham sido compromissados. Isso apontou que a folha de pagamento fora um alvo deliberado. Maior que um ataque ao acaso. Indícios apontaram que o ataque foi provavelmente cometido por um funcionário (alguém que teria conhecimento do sistema) que se beneficiaria com a modificação de dados dentro dele. A investigação foi bastante difícil e a recuperação do sistema bastante dolorosa.

Fonte: 2002 Australian Computer Crime and Security Survey.

Contribuem para a perda da integridade: as inserções, substituições ou exclusões de parte do conteúdo da informação; as alterações nos seus elementos de suporte, que podem ocorrer quando são realizadas alterações na estrutura física e lógica onde ela está armazenada, ou quando as configurações de um sistema são alterados para se ter acesso a informações restritas, bem como são superadas as barreiras de segurança de uma rede de computadores.

Disponibilidade

A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 27002:2005).

Ocorre a quebra da disponibilidade quando a informação não está disponível para ser utilizada, ou seja, ao alcance de seus usuários e destinatários, não podendo ser acessada no momento em que for necessário

[1] Fonte: 2002 Australian Computer Crime and Security Survey. Pesquisa produzida conjuntamente pelos AusCERT, Deloitte Touche Tohmatsu e NSW Police.

[2] Tradução e adaptação do texto original pelo autor.

utilizá-la. Garantir a disponibilidade é assegurar o êxito da leitura, do trânsito e do armazenamento da informação.

Sabotagem na GreenGrocer.com.au[3]

Em março de 2000, a Unidade de investigação de crime de informática da agência de crime comercial (NSW Police) investigou um ataque de sabotagem contra a rede de trabalho de uma loja de hortifrutigranjeiros (GreenGrocer's network), o qual a fez falhar em duas ocasiões. Em um dos ataques, foram deletados arquivos de sistemas, causando a indisponibilidade por cinco dias.

Como integrante do e-commerce, esse ataque foi crítico e afetou a capacidade de atender clientes e obter ganhos. Na ocasião, o prejuízo foi de $ 22,500 por dia.

Como resultado, a companhia prestou uma queixa ao NSW Police. Uma trilha de auditoria mostrou uma conexão remota imediatamente anterior a dois incidentes originados de endereços IP pertencentes a um consumidor, que foi identificado como um antigo engenheiro da rede de trabalho de informática da GreenGrocer, o qual tinha sido demitido dias antes, após uma disputa por uma cargo de gerente.

Análises de investigações mostraram que o agressor tinha, na primeira ocasião, invadido a rede de trabalho da GreenGrocer e deletado arquivos que levaram a perda da sua conexão com a internet. No segundo ataque, o invasor acessou remotamente um servidor e deletou arquivos de operações críticas do sistema, o que causou a falha do servidor. O agressor efetuou ataques utilizando o serviço de acesso remoto, que foi habilitado durante o período em que ele esteve no emprego.

O caso destaca a importância de se adotarem controles com relação ao pessoal, tais como desabilitar contas de funcionários demitidos com nível de acesso privilegiado, e a necessidade de monitorar o maior serviço de acesso remoto quando eles forem solicitados.

O agressor foi preso em fevereiro de 2002 e sentenciado à pena máxima de 10 anos de prisão, de acordo com a Lei (NSW Crimes Act 1900), mas recebeu a suspensão da pena em 18 meses.

Fonte: 2002 Australian Computer Crime and Security Survey.

Confidencialidade

A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso (NBR ISO/IEC 27002:2005).

[3] Tradução e adaptação do texto original pelo autor.

Ocorre a quebra da confidencialidade da informação ao se permitir que pessoas não autorizadas tenham acesso ao seu conteúdo. A perda da confidencialidade é a perda do segredo da informação. Garantir a confidencialidade é assegurar o valor da informação e evitar a divulgação indevida.

Perdas financeiras por vazamento de informações[4]

Em um caso recente, um cliente de uma empresa australiana descobriu que suas informações estratégicas e de grande valor confidencial tinham sido vazadas para um concorrente. O vazamento foi a fonte de considerável sentimento de culpa e perdas financeiras, não apenas para o cliente da empresa mas para o serviço dela, que estava encarregado da proteção da informação antes de seu vazamento. Com o objetivo de preservar a relação e a reputação com seus clientes, foi conduzida uma investigação para determinar a causa e a fonte do vazamento. Agências da Lei também foram envolvidas na investigação.

A investigação mostrou que um empregado falhou ao não seguir o padrão de proteção adotado para documentos confidenciais. O beneficiado, ou alguém dentro da empresa beneficiada (concorrente), percebendo a importância das informações, vazou essas informações para o concorrente.

O uso indevido da tecnologia de informação conduziu para brechas de segurança e, consequentemente, para o vazamento de informações confidenciais.

O caso demonstrou que questões de negligência têm afetado muitas empresas, contribuindo para suas perdas inestimáveis.

Fonte: 2002 Australian Computer Crime and Security Survey.

Com a evolução da área de segurança da informação, observa-se a preocupação com outras propriedades, mais precisamente em relação ao processo de comunicação, pois a **NBR ISO/IEC 17799:2001** estabelecia que a segurança da informação estava caracterizada pela preservação da confidencialidade, da integridade e da disponibilidade da informação. Já a **NBR ISO/IEC 27002:2005** mantém esse conceito, acrescentando que outras propriedades podem também estar envolvidas, tais como: a autenticidade, a responsabilidade, o não repúdio e a confiabilidade.

Autenticidade: é a garantia de que a informação é oriunda da fonte que lhe é atribuída e elaborada por quem tem autoridade para tal.

[4] Tradução e adaptação do texto original pelo autor.

Confiabilidade: é a garantia de que a informação é confiável, oriunda de uma fonte autêntica e que expressa uma mensagem verdadeira.
A autenticidade e confiabilidade estão interligadas. A primeira diz respeito à idoneidade da fonte, isto é, digna de fé e confiança, e a segunda ao seu conteúdo. A avaliação da fonte para a sua autenticidade pode ser feita com relação à sua idoneidade, como, por exemplo: completamente idônea, regularmente idônea, inidônea e cuja idoneidade não se pode avaliar. E a avaliação da confiabilidade pode ser feita com relação ao seu conteúdo, como, por exemplo: confirmação por outras fontes, por ser verdadeira, duvidosa ou improvável.

Não repúdio: é a garantida de que a informação chegará ao destino certo e não será repudiada.

Responsabilidade: é a coparticipação de responsabilidades por todos os que produzem, manuseiam, transportam e descartam a informação, seus sistemas e redes de trabalho.

Dessa forma, a autenticidade do emissor é a garantia de que quem se apresenta como remetente é realmente quem diz ser. A confiabilidade é a garantia de que a informação está completa e igual à sua forma original quando do envio pelo remetente, e expressa uma verdade. O não repúdio é a garantia de que o emissor ou receptor não tem como alegar que a comunicação não ocorreu, e a responsabilidade diz respeito aos deveres e proibições entre remetente e destinatário.

1.2 Classificações da informação

A classificação da informação contribui para a manutenção das principais características da informação (confidencialidade, integridade e disponibilidade). A NBR ISO 27002:2005 não estabelece classificação para as informações, apenas recomenda que a informação seja classificada considerando-se o seu valor, requisitos legais, sensibilidade e criticidade para a organização.

O Decreto Federal nº 4.553/2002,[5] que disciplina, no âmbito da administração pública federal, a salvaguarda de dados, informações, documentos e materiais sigilosos, estabelece em seu art. 2º, que são considerados sigilosos os dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco para a segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas, e o seu acesso é restrito e condicionado à necessidade de conhecer.

Esse decreto, em seu Art. 5º, classifica os dados ou informações quanto ao grau de sigilo[6] em quatro categorias: **Ultrassecretos**: aqueles cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado; **Secretos**: aqueles cujo conhecimento não autorizado possa causar dano grave à segurança da sociedade e do estado; **Confidenciais**: aqueles que, no interesse do poder executivo e das partes, devam ser de conhecimento restrito, e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado; e **Reservados**: aqueles cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

Abaixo, a reprodução do Art. 5º do Decreto 4.553/2002:

> Art. 5º Os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos.
>
> § 1º São passíveis de classificação como ultra-secretos, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa

[5] Esse Decreto dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal.

[6] O grau de sigilo é a gradação atribuída a dados, informações, área ou instalação, considerados sigilosos em decorrência de sua natureza ou conteúdo.

> acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.
>
> § 2º São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.
>
> § 3º São passíveis de classificação como confidenciais dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.
>
> § 4º São passíveis de classificação como reservados dados ou informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

Verifica-se que é mais comum a classificação da informação quanto ao sigilo; contudo, essa classificação pode ser efetuada com base em outros critérios, como, por exemplo, para atender aos requisitos de confidencialidade, integridade e disponibilidade. E essa é a linha adotada por Beal (2005).

As classificações propostas por Beal dentro dos **requisitos de confidencialidade** são: **confidencial**: toda informação cuja divulgação para pessoas não autorizadas pode causar danos graves à organização; **reservada**: informações que no interesse da organização devem ser de conhecimento restrito e cuja revelação não autorizada pode frustrar o alcance de objetivos e metas; e **pública**: informações de livre acesso. Para os **requisitos de disponibilidade**, orienta que a informação deve ser classificada de acordo com o impacto que a sua falta pode provocar para a empresa, podendo ser estabelecidas categorias para o tempo de recuperação (de minutos a semanas). Exemplifica, classificando-as por tempo de recuperação em: curto,

médio, sem exigência e com exigência (sazonalidade). Para os **requisitos de integridade,** classifica as informações em alta, média e baixa exigência de integridade. Apresenta, ainda, a classificação para atender aos **requisitos de autenticidade**, classificando-as quanto à exigência da verificação da autenticidade ou não, que podem ser, por exemplo, informações que devem ter a sua procedência confirmada antes da utilização, como no caso de um pedido de criação de senha de acesso a um sistema de informação.

Outra classificação que pode ser feita é com relação ao grau de importância dos dados para os principais processos de negócios e o custo para a sua recuperação no caso da ocorrência de um evento ou desastre. E essa é a linha adotada por Toigo (2003), que classifica os dados em **crítico**, **vital**, **sensível** e **não sensível**.

Abaixo a classificação adotada por Toigo:[7]

Crítico: dados ou documentos que devem ser mantidos por razões legais, para uso nos processo-chaves dos negócios, ou para uma mínima restauração aceitável nos níveis de trabalho em um evento ou desastre.

Vital: dados ou documentos que devem ser mantidos para uso nos processos normais, e que representam um investimento substancial de recursos da companhia, que podem dificultar ou impossibilitar a sua recuperação, mas que podem não ser necessários numa situação de recuperação de desastre. Informações que necessitam de sigilo especial podem ser incluídas nessa categoria.

Sensível: dados ou documentos que devem ser necessários nas operações normais, mas para os quais existem fornecimentos alternativos disponíveis em um evento de perda. Dados que podem ser reconstruídos rapidamente, por completo, mas que possuem algum custo, podem ser classificados nessa categoria.

Não crítico: dados ou documentos que podem ser reconstruídos facilmente com custo mínimo, ou cópias de dados críticos, vitais e sensíveis, que não necessitem de pré-requisitos de proteção.

Um outro esquema de classificação pode ser feito considerando-se os níveis estratégico, tático e operacional da empresa. Essa opção poderia considerar, por exemplo, que as informações do nível estratégico sejam

[7] Tradução e adaptação por conta do autor.

classificadas como confidenciais (críticas ou vitais), as do nível tático como restritas (sensíveis), e as do nível operacional como sensível (algumas) e públicas ou ostensivas (não críticas).

Como pode ser visto, a classificação tende a variar de organização para organização, sejam elas públicas ou privadas, cuja diferença está no critério a ser adotado. No geral, a classificação da informação objetiva assegurar um nível adequado de proteção, e o importante é que seja feita uma classificação que objetive preservar os requisitos fundamentais estabelecidos pela organização para a segurança das informações durante o seu ciclo de vida.

1.3 Ciclo de vida da informação

A informação possui um ciclo de vida. Ela nasce com a produção, tem um tempo de vida útil, na qual é manuseada, utilizada interna e externamente, transportada por diversos meios, armazenada, e morre com a sua destruição.

A doutrina tem apresentado o seguinte ciclo de vida para as informações: produção e manuseio, armazenamento, transporte e descarte. A produção é a fase na qual nasce a informação, e o manuseio, como o próprio nome já o diz, é o ato de manusear a informação. É nessa fase que se caracteriza a materialização do conhecimento; O transporte é a fase da condução por quaisquer meios nos quais conste a informação. O armazenamento é o ato de arquivar as informações. E o descarte é o ato de descartar ou inutilizar a informação.

Alguns autores, como Beal (2005), apresentam mais algumas etapas para o ciclo de vida da informação. Beal apresenta seis etapas: identificação das necessidades e dos requisitos, obtenção, tratamento, distribuição, uso, armazenamento e descarte.

A identificação das necessidades e dos requisitos, para Beal, é o ponto de partida do ciclo de vida da informação, por entender que essa etapa age como um elemento acionador de todo o processo, podendo vir a estabelecer um ciclo contínuo de coleta. Ela enfatiza que a recompensa por descobrir essas demandas se dá ao tornar a informação mais útil e os seus destinatários mais receptivos à sua utilização. Na etapa da obtenção, são desenvolvidas as

atividades de criação, recepção ou captura de informação proveniente de fonte externa ou interna. Na etapa do tratamento, caracteriza a passagem da informação por processos para torná-la mais acessível, organizada e fácil de localizar pelos usuários.

Verifica-se que a classificação de Beal aproxima-se mais de um esquema de produção do conhecimento, pois a identificação das necessidades e requisitos é parte integrante da fase do planejamento, que é uma das etapas da produção do conhecimento.

Independentemente da linha a ser adotada, todas essas etapas do ciclo de vida da informação são importantes para o ciclo de produção do conhecimento.

1.4 Ciclo de produção do conhecimento

Como já foi abordado, o conhecimento resulta de um processamento de dados, informações e conhecimentos anteriores, que são avaliados, analisados, interpretados e compreendidos dentro de um contexto, a fim de serem utilizados numa ou mais aplicações específicas. Esse processo de produção do conhecimento passa pelas seguintes fases: planejamento, reunião, análise, interpretação, formalização e difusão.

O **planejamento** constitui a fase inicial, pois é nela que se decide o que se quer fazer, como fazer e para que fazer. É nessa fase que se identificam as principais fontes de dados, sejam elas internas e externas. A **reunião** caracteriza-se pela coleta dos dados já disponíveis pela pessoa e pela ação de campo para a obtenção de novos dados. A **análise** é a fase na qual se avaliam os dados obtidos e se faz a interligação com os dados de outras fontes. A **interpretação** do analista é uma operação intelectual, na qual ele concebe ideias, formula juízos de valor sobre um conjunto de dados, o que resulta na produção do conhecimento. As últimas fases são a **formalização e difusão** do conhecimento produzido, que poderá ser destinado ao público interno e/ou ao mercado.

Todas as fases são importantes na produção do conhecimento, porém, se o analista não tiver um bom raciocínio, o conhecimento tornar-se-á fragilizado e o resultado poderá não ser aquele desejado.

Após a produção do conhecimento, ele serve para satisfazer as demandas, como também pode gerar novas necessidades de conhecimento, as quais servirão para orientar uma nova produção do conhecimento.

Observa-se que a produção é um sistema cíclico, pois essa nova orientação pode ser considerada como um *feedback* para a retroalimentação do sistema de produção do conhecimento, como está demonstrado abaixo:

ESQUEMA SIMPLIFICADO DO CILCO DE PRODUÇÃO DO CONHECIMENTO

Fonte: Dantas (2011)

1.5 A informação como um ativo

O estudo do ativo não é uma preocupação recente, pois há muito tempo a ciência da contabilidade já o estudava. A definição clássica é que o ativo compreende o conjunto de bens e direitos de uma entidade. Entretanto, atualmente, um conceito mais amplo tem sido adotado para se referir ao ativo como tudo aquilo que possui valor para a empresa.

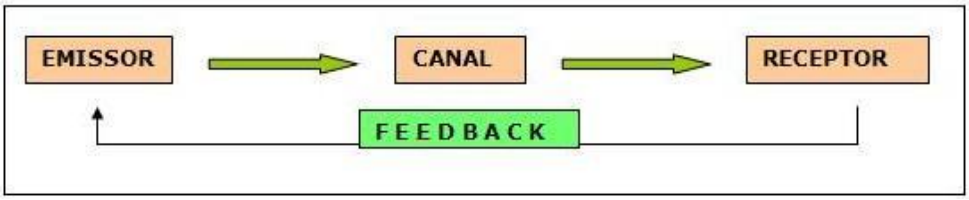
Ativo: qualquer coisa que tenha valor para a organização (ISO/IEC 13335-1:2004).

Como a informação tem ocupado um papel de destaque no ambiente de negócios, e também tem adquirido um potencial de valoração para as organizações e para as pessoas, ela passou a ser considerada o seu principal ativo.

Entretanto, para se proteger a informação, mantendo os requisitos de segurança (confidencialidade, integridade e disponibilidade), deve-se atentar para o processo de comunicação. E para que a informação seja protegida durante todo esse processo, não basta tê-la como um componente a proteger, mas também devem ser considerados os outros elementos que fazem parte desse processo, que são, por exemplo: os sistemas, os aplicativos, os equipamentos, os serviços e as pessoas que os utilizam.

O processo de comunicação está representado na figura abaixo, onde a informação parte de um emissor, que é aquele que codifica a mensagem, sendo transmitida por um canal de comunicação, até chegar a seu receptor, que é aquele que decodifica a mensagem, fornecendo o *feedback* ao emissor.

ESQUEMA SIMPLIFICADO DO PROCESSO DE COMUNICAÇÃO



Fonte: Dantas (2011)

Nesse processo, existem três elementos que merecem especial atenção: a informação, os equipamentos que lhe oferecem suporte e as pessoas que a utilizam.

As **informações** são: os documentos, relatórios, livros, manuais, correspondências, patentes, informações de mercado, código de programação, linhas de comando, arquivo de configuração, planilha de remuneração de funcionários, plano de negócios de uma empresa, etc.

Os elementos que oferecem suporte às informações podem ser divididos em três grupos: *software, hardware* e organização.

Os **softwares** compõem o grupo dos programas de computador utilizados para a customatização de processos, ou seja, o acesso, a leitura, o trânsito e o armazenamento da informação. São constituídos pelos aplicativos comerciais, programas institucionais, sistemas operacionais, programas de correio eletrônico, sistemas de suporte.

Os **hardwares** representam toda a infraestrutura tecnológica que oferece suporte à informação. São quaisquer equipamentos em que se processe, transmita e armazene a informação. São os computadores, os servidores, os *mainframes*, os meios de armazenamento, os equipamentos de conectividade, roteadores, *switchs*, e qualquer outro elemento de uma rede de computadores através do qual sejam transmitidas informações.

A **organização** é toda a estrutura organizacional, a saber, a sua estrutura departamental e funcional, o quadro de alocação dos funcionários, a distribuição de funções e os fluxos de informação da empresa. O ambiente físico compõe as salas, os armários onde são colocados os documentos, a infoteca, a sala de servidores e o arquivo.

E as **pessoas** são todos aqueles que, de uma forma ou outra, lidam com a informação ao utilizarem a estrutura tecnológica e de comunicação da empresa.

A NBR ISO/IEC 27002:2005 exemplifica como ativos associados aos sistemas de informação: **ativos de informação**: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas; **ativos de software**: aplicativos, sistemas de uma forma geral, ferramentas de desenvolvimento e utilitários; **ativos físicos**: equipamentos computacionais (processadores, monitores, *laptops*, modens), equipamentos de comunicação (roteadores, PABXs, fax, secretárias eletrônicas), mídia magnética (fitas e discos), mídias removíveis e outros equipamentos técnicos (*no-breaks*, ar-condicionado), mobília, acomodações; e **serviços**: computação e serviços de comunicação, utilidades gerais, por exemplo: aquecimento, iluminação, eletricidade, refrigeração; **pessoas**: pessoas e suas qualificações, habilidades e experiências; **intangíveis**: reputação e imagem da organização

Para a segurança da informação, é fundamental a identificação dos elementos que compõem o processo de comunicação para se identificarem as vulnerabilidades da informação.

1.6 Vulnerabilidades da informação

Vulnerabilidades são fragilidades que de alguma forma podem vir a provocar danos. A NBR ISO/IEC 27002:2005 define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Beal (2005) define a vulnerabilidade como uma fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque.

Para Sêmola (2003), as vulnerabilidades são fragilidades presentes ou associadas a ativos de informação, que, ao serem exploradas, permitem a ocorrência de incidente na segurança da informação.

Dantas (2003) afirma que vulnerabilidades são fragilidades que podem provocar danos decorrentes da utilização de dados em qualquer fase do ciclo de vida das informações.

Como pode ser verificado, as vulnerabilidades estão relacionadas diretamente com as fragilidades. Essas fragilidades podem estar nos processos, políticas, equipamentos e nos recursos humanos. Por si só, elas não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou de condição favorável, já que se trata de ameaças.

De acordo com as análises feitas nas pesquisas realizadas pela Módulo Security S.A., nos anos de 2003 e 2004, foram identificados alguns pontos que demonstram uma relação direta com as vulnerabilidades para a segurança das informações.

VULNERABILIDADES	**2002**	**2003**
Principais pontos de invasão		
Internet	55%	60%
Sistemas internos	20%	23%
Principais responsáveis		
Hackers	48%	32%
Funcionários	24%	23%
Prestadores de serviços	12%	4%
Principais obstáculos para a implementação da segurança da informação		

Falta de consciência dos executivos	33%	23%
Falta de consciência dos usuários	29%	14%

Fonte: Dantas (2011)

A internet foi, para 60% das empresas pesquisadas, o principal ponto de invasão, o que demonstra que essa tecnologia tem contribuído para o aumento das vulnerabilidades.

Outro ponto que desperta a atenção é que, apesar da evolução da segurança da informação, os ataques ainda permanecem em patamar preocupante. Segundo dados da pesquisa *2006 Australian Computer Crime and Security Survey* (AusCERT, 2006), os ataques *trojan* e *phishing* tiveram um crescimento de 27% em relação ao ano de 2005. Já para o CSI/FBI (2006), os vírus ainda permanecem como a principal fonte de grandes perdas financeiras, seguido do acesso não autorizado.

Outro ponto de vulnerabilidade apresentado nas pesquisas sobre segurança da informação tem relação com os funcionários e prestadores de serviço. Sabemos que a fuga das informações e a sua exposição involuntária ocorrem em momentos simples do dia a dia da empresa, o que torna os recursos humanos uma das maiores preocupações para a implementação de políticas e treinamentos voltados para a proteção das informações.

Tudo isso demonstra o quanto existe de vulnerabilidade no ambiente de negócios, bem como o tamanho da preocupação dos especialistas em segurança da informação com o crescimento da tecnologia.

É certo que ela torna a vida mais prática e as informações mais acessíveis, proporcionando conforto, economia de tempo e segurança. Mas, essa aparente segurança não é motivo de tranquilidade, pois a ausência de uma cultura da segurança das informações cria um ambiente vulnerável às informações, porque os mesmos benefícios que a tecnologia oferece são também utilizados para a prática de ações danosas às empresas, como pôde ser visto nos argumentos apresentados acima.

Origem das vulnerabilidades

As vulnerabilidades podem advir de vários aspectos: instalações físicas desprotegidas contra incêndio, inundações e desastres naturais; material inadequado empregado nas construções; ausência de políticas de segurança

para RH; funcionários sem treinamento e insatisfeitos nos locais de trabalho; ausência de procedimentos de controle de acesso e de utilização de equipamentos por pessoal contratado; equipamentos obsoletos, sem manutenção e sem restrições para sua utilização; *software* sem *patch* de atualização e sem licença de funcionamento, etc.

Para uma melhor compreensão das vulnerabilidades, podemos classificá-las como: naturais, organizacionais, físicas, de *hardware*, de *software*, nos meios de armazenamento, humanas e nas comunicações.

Naturais

As vulnerabilidades naturais estão relacionadas com as condições da natureza ou do meio ambiente que podem colocar em risco as informações. Podem ser: locais sujeitos a incêndios em determinado período do ano; locais próximos a rios propensos a inundações; áreas onde se verificam manifestações da natureza, como terremotos, maremotos e furacões; falha geológica, zonas de inundação, áreas de desmoronamento e avalanches.

Organizações situadas nessas áreas vulneráveis devem manter um excelente gerenciamento de continuidade de negócios, uma vez que esses eventos independem de previsibilidade e da vontade humana.

Organizacional

As vulnerabilidades de origem organizacional dizem respeito a políticas, planos e procedimentos, e a tudo mais que possa constituir a infraestrutura de controles da organização e que não seja enquadrado em outras classificações. Podem ser: ausência de políticas de segurança e treinamento; falhas ou ausência de processos, procedimentos e rotinas; falta de planos de contingência, recuperação de desastres e de continuidade; ausência ou deficiência da CIPA (Comissão Interna de Prevenção de Acidentes), etc.

Física

As vulnerabilidades físicas dizem respeito aos ambientes em que estão sendo processadas ou gerenciadas as informações. Podem ser: instalações inadequadas; ausência de recursos para combate a incêndio; disposição desordenada dos cabos de energia e de rede; não identificação de pessoas e

locais; portas destrancadas; acesso desprotegido às salas de computador; sistema deficiente de combate a incêndio; edifícios mal projetados e mal construídos; material inflamável utilizado na construção e no acabamento; janelas destrancadas; paredes suscetíveis a um assalto físico; paredes que não vão até o teto (meia parede).

Hardware

Caracterizam-se como vulnerabilidade de *hardware* os possíveis defeitos de fabricação ou configuração dos equipamentos que podem permitir o ataque ou a alteração dos mesmos. Como exemplo desse tipo de vulnerabilidade, temos: a conservação inadequada dos equipamentos; a falta de configuração de suporte ou equipamentos de contingência; *patches* ausentes; *firmware* desatualizado; sistemas mal configurados; protocolos de gerenciamento permitidos por meio de interfaces públicas.

Software

As vulnerabilidades de *software* são constituídas por todos os aplicativos que possuem pontos fracos que permitem acessos indevidos aos sistemas de computador, inclusive sem o conhecimento de um usuário ou administrador de rede. Os principais pontos de vulnerabilidade encontrados estão na configuração e instalação indevida, programas, inclusive o uso de *e-mail,* que permitem a execução de códigos maliciosos, editores de texto que permitem a execução de vírus de macro.

Ataque *trojan*[8]

Em janeiro de 2001, nos Estados Unidos, uma pessoa comunicou aos aplicadores da lei daquele país que um *hacker*, localizado na Austrália, tinha obtido acesso ao seu computador via cabo *modem*. **A vítima tinha instalado um software antivírus no final de 1999, mas não o tinha atualizado desde aquela época**. A vítima alegou que o invasor descreveu o que ele estava usando via *web cam*, bem como acessou, deletou e modificou arquivos no seu computador.

Análise forense no computador da vítima revelou a presença do *SubSeven trojan*. O *trojan* fora colocado no sistema da vítima desde maio de 2000. **Um firewall foi instalado no sistema da vítima em outubro de 2000, mas o invasor manteve o acesso ao computador da vítima apesar dessa ferramenta de prevenção.** O *trojan* foi

[8] Tradução e adaptação do texto original pelo autor.

configurado para notificar o atacante no canal IRC *Chat* quando a vítima estava *on-line*, e no seu endereço IP.
Fonte: 2002 Australian Computer Crime and Security Survey.

Meios de armazenamento

Os meios de armazenamento são todos os suportes físicos ou magnéticos utilizados para armazenar as informações, tais como: disquetes; CD ROM; fita magnética; discos rígidos dos servidores e dos bancos de dados; tudo o que está registrado em papel.

As suas vulnerabilidades advêm de prazo de validade e expiração, defeito de fabricação, utilização incorreta, local de armazenamento em áreas insalubres ou com alto nível de umidade, magnetismo ou estática, mofo, etc.

Humanas

As vulnerabilidades humanas constituem a maior preocupação dos especialistas, já que o desconhecimento de medidas de segurança é a sua maior vulnerabilidade.

Sua origem pode ser: falta de capacitação específica para a execução das atividades inerentes às funções de cada um; falta de consciência de segurança diante das atividades de rotina; erros; omissões; descontentamento; desleixo na elaboração e segredo de senhas no ambiente de trabalho; não utilização de criptografia na comunicação de informações de elevada criticidade, quando possuídas na empresa.

Funcionários deixam vazar informações confidenciais
21% largam documentos em impressoras, afirma pesquisa
Vazamentos de informações privilegiadas como no caso da compra do grupo Ipiranga por Petrobras, Braskem e Ultra, o que motivou investigações da CVM, têm sido bastante corriqueiros no cenário empresarial e muitos ocorrem por práticas até inocentes de funcionários.
Enquanto as empresas investem em tecnologias para proteger seus dados confidenciais de ataques externos, eles têm escapado pelas mãos de pessoas ligadas à própria companhia. A conclusão é de estudo da empresa de tecnologia de segurança da informação McAfee, feito pela pesquisadora Illuminas, que entrevistou, nos EUA, organizações com mais de 200 funcionários, em janeiro.
Apesar de a pesquisa ter sido feita com companhias americanas, o cenário pode ser seguramente aproximado do brasileiro, segundo José Antunes, responsável pela área

de engenharia de sistemas da McAfee.
Dentre os entrevistados, 84% dizem que suas empresas têm políticas para informações sigilosas, como bloqueios e senhas. Apesar disso, o levantamento indicou que elas são facilmente desrespeitadas pelos funcionários. Cerca de 21% assumiram que deixam documentos confidenciais ou reservados na bandeja de saída da impressora. E 26% não fragmentam documentos confidenciais quando terminam de trabalhar.
Até dez documentos são retirados por semana do escritório em dispositivos portáteis por 38% dos questionados. Os meios de saída são *laptops*, levados por 41%; memórias USB, por 22%, e CD-ROM, por 13%.
O levantamento também verificou que 22% admitiram que, às vezes, emprestam a colegas os dispositivos onde armazenam documentos de trabalho.
"O modo como o dado sai da empresa é semelhante em todo o mundo", diz Antunes. Ele cita o caso da Ipiranga. "Aí está claro que houve informação privilegiada. Provavelmente não foi de alguém que tinha noção do risco. Quem tem poder sabe que pode custar caro."
Uma outra pesquisa semelhante, realizada com 350 empresas de grande porte no Brasil, feita pela Via Fórum - que organiza o evento sobre segurança da informação Security Week Brasil-, mostra que 54% das questionadas já tiveram suas redes, servidores ou computadores atacados. Dentre elas, 40% dizem que os incidentes partiram de dentro da empresa.
Comparando companhias americanas e brasileiras, Antunes diz que aqui a violência produz agravantes. "Um laptop nunca deve carregar dados sigilosos pelo risco de assalto. O ladrão pode nem estar procurando isso, mas acaba vendendo o equipamento sem apagar os arquivos e as informações podem cair em mãos erradas. Se precisar sair da empresa, é melhor levar o dado no USB."
Fonte: http://www1.folha.uol.com.br/fsp/dinheiro/fi0605200721.htm

Comunicação

Nas comunicações, as vulnerabilidades incluem todos os pontos fracos que abrangem o tráfego das informações, por qualquer meio (cabo, satélite, fibra óptica, ondas de rádio, telefone, internet, *wap*, fax, etc.).

Os principais aspectos estão relacionados com: a qualidade do ambiente que foi preparado para o tráfego, tratamento, armazenamento e leitura das informações; a ausência de sistemas de criptografia nas comunicações; a má escolha dos sistemas de comunicações para o envio da mensagem; os protocolos de rede não criptografados; as conexões a redes múltiplas; os

protocolos desnecessários permitidos; a falta de filtragem entre os segmentos da rede.

Ataque *trojam* em *site* de universidade[9]
Uma universidade australiana relatou para os aplicadores da lei que uma máquina da sua *network* tinha sido comprometida por um **ISP Australiano, e utilizada como base para atividade hacker com outras 70 máquinas** de instituições acadêmicas ao redor do mundo, por um período de duas semanas.
O atacante instalou um trojan secure Shell (ssh) no sistema da primeira universidade, admitindo uma conexão para a máquina e atingindo outros controles. **Muitos dos sistemas atingidos (vítimas secundárias) possuíam uma configuração precária, como ausência de partes e rotinas de registro, além da falta de monitoramento de seus sistemas.**
Fonte: 2002 Australian Computer Crime and Security Survey.

1.7 Ameaças à segurança da informação

No ambiente atual, bastante competitivo, as empresas devem estar sempre atentas para as ameaças aos negócios corporativos, que, se concretizadas poderão tirá-las desse cenário, encerrando suas atividades para sempre.

Com a automação dos sistemas de processamento e de armazenamento de informações, a própria informação torna-se mais susceptível às ameaças, uma vez que ela (a informação) está mais acessível e disponível para usuários de uma forma geral.

Mas, o que são ameaças?

Ameaças são agentes ou condições que, ao explorarem as vulnerabilidades, podem provocar danos e perdas.

A norma ISO/IEC 13335-1:2004 define ameaças como: **a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização.**

Sêmola (2003) define ameaças como sendo agentes ou condições que causam incidentes que comprometem as informações e seus ativos, por meio de exploração de vulnerabilidades, o que provoca perdas de confiabilidade,

[9] Tradução e adaptação do texto original pelo autor.

integridade e disponibilidade, e, consequentemente, causando impactos aos negócios de uma organização.

Para Beal (2005), ameaças são expectativas de acontecimento acidental ou proposital, causado por agente, o qual pode afetar um ambiente, sistema ou ativo de informação.

Observa-se que as vulnerabilidades estão relacionadas com situações de fragilidade existentes no ambiente ou nos ativos, e que elas estão relacionadas com um incidente indesejado que, em decorrência daquela, pode vir a provocar algum dano.

Essas ameaças podem surgir de várias formas: de eventos da natureza, como terremotos, furacões, enchentes, descargas elétricas, *tsunamis*, etc; de incidentes em instalações, como incêndio, curtos-circuitos, infiltrações; de incidentes de segurança, com roubo, furto, sabotagem, ataques terroristas, etc; e de uma variedade de eventos, que, de uma forma ou de outra, pode vir a afetar os negócios de uma organização.

As ameaças podem ser: **naturais:** são aquelas que se originam de fenômenos da natureza, tais como terremotos, furacões, enchentes, maremotos, *tsunamis*; **involuntárias:** são as que resultam de ações desprovidas de intenção para causar algum dano. Geralmente são causadas por acidentes, erros, ou por ação inconsciente de usuários, tais como vírus eletrônicos, que são ativados pela execução de arquivo anexado às mensagens de *e-mail*; e **intencionais:** são aquelas deliberadas, que objetivam causar danos, tais como *hackers*, fraudes, vandalismo, sabotagens, espionagem, invasões e furtos de informações, dentre outras.

Fontes de diversas origens apresentam tipos de ameaças à informação, contudo, o ponto referencial mais confiável são as pesquisas sobre segurança da informação, as quais apresentam as principais ameaças que permeiam o ambiente das informações.

Dentre as pesquisas sobre segurança da informação, sem prejuízo de outras fontes, destacamos as realizadas pela Módulo Security Solutions, as realizadas pelo Computer Security Institute (CSI), juntamente com o Federal Bureau of Investigation (FBI), as da Ernst & Young, pela Deloitte Touche Tohmatsu, e as efetuadas pela Australia's National Computer Emergency Response Team (AusCERT), em conjunto com outros órgãos de combate aos crimes de informática e computador da Austrália.

Abaixo apresentamos os principais destaques de duas pesquisas nacionais sobre segurança da informação:

8ª Pesquisa nacional de segurança da informação

Principais destaques

- 43% das empresas entrevistadas sofreram ataques nos últimos 12 meses, o que representa um aumento de 10% em relação a 2001, sendo que 24% nos últimos 6 meses.
- 78% das empresas no Brasil reconhecem que tiveram perdas financeiras, porém, 56% ainda não conseguem quantificar o valor dos prejuízos causados pelos problemas com a segurança da informação. Em 22% das organizações que conseguiram contabilizar esses valores, o total de perdas registradas foi de R$ 39,7 milhões.
- Os *hackers* (48%) foram os maiores responsáveis por ataques e invasões em 2002, o que significa um aumento de 15% com relação a 2001.
- A Internet continua sendo considerado o principal ponto de ataque com 55%. No entanto, o acesso remoto teve o maior aumento, passando de 9% em 2001 para 16% em 2002, um aumento de 78% em apenas 1 ano.
- 82% dos entrevistados acreditam no aumento dos problemas relacionados com a segurança da informação.
- Das medidas de segurança adotadas, a análise de riscos teve o maior aumento com relação à pesquisa anterior, passando de 24% em 2001 para 53% em 2002.
- Somente 36% das empresas possuem um plano de ação formalizado no caso de um eventual ataque ou invasão.
- A segurança da informação passou a ser um fator importante para 45% dos executivos, sendo que 16% a consideram crítica e 32% a entendem como sendo vital. Mesmo assim, a falta de conscientização dos executivos (45%) e dos usuários (38%) foi apontada como o principal obstáculo para a implementação da segurança nas corporações.
- 77% dos profissionais entrevistados informaram que suas empresas pretendem aumentar os investimentos em segurança em 2003.
- 78% das empresas possuem orçamento específico para a área de segurança da informação, sendo que 33% alocam recursos entre 1 e 5% do orçamento total de tecnologia, e 24% alocam de 5 a 10%.
- A área de tecnologia ainda é a responsável pela segurança da informação em 41% das empresas participantes da pesquisa. Em seguida, vem a área de *Security Office,* com 31%. Em 12% das organizações, ainda não há uma área

especifica para tratar a questão de segurança da informação.

- 98% das empresas pesquisadas possuem pelo menos 1 pessoa dedicada à segurança da informação, sendo que 24% delas possuem mais de 10 pessoas dedicadas.
- 81% das empresas pretendem investir em capacitação da equipe técnica. 30% dos entrevistados alocam de 1 a 5% do orçamento total da empresa para a área de tecnologia da informação.
- 36% das empresas ainda não possuem um planejamento dedicado à segurança da informação.
- 66% dos usuários deixam de comprar pela Internet por causa da sensação de falta de segurança.

Fonte: 8ª Pesquisa nacional de segurança da informação.

9ª Pesquisa nacional de segurança da informação

Principais destaques

Para 78% dos entrevistados, as ameaças, os riscos e os ataques deverão aumentar em 2004.

42% das empresas tiveram problemas com a segurança da informação nos seis meses anteriores à pesquisa.

35% das empresas reconhecem que tiveram perdas financeiras. Já o percentual de empresas que não conseguiram quantificar essas perdas diminuiu de 72% em 2002 para 65% em 2003.

Vírus (66%), funcionários insatisfeitos (53%), divulgação de senhas (51%), acessos indevidos (49%) e vazamento de informações (47%) foram apontados como as cinco principais ameaças à segurança das informações nas empresas.

O percentual de empresas que afirmam ter sofrido ataques e invasões subiu de 43% em 2002 para 77% em 2003.

32% dos entrevistados apontam os *hackers* como os principais responsáveis por ataques e invasões de sistemas corporativos.

26% das empresas não conseguem sequer identificar os responsáveis pelos ataques.

48% não possuem nenhum plano de ação formalizado em caso de invasões e ataques.

60% indicam a internet como principal ponto de invasão em seus sistemas.

58% dos entrevistados sentem-se inseguros para comprar em *sites* de comércio eletrônico por causa da sensação de falta de segurança.

A falta de consciência dos executivos é apontada por 23% dos entrevistados como o principal obstáculo para a implementação da segurança.

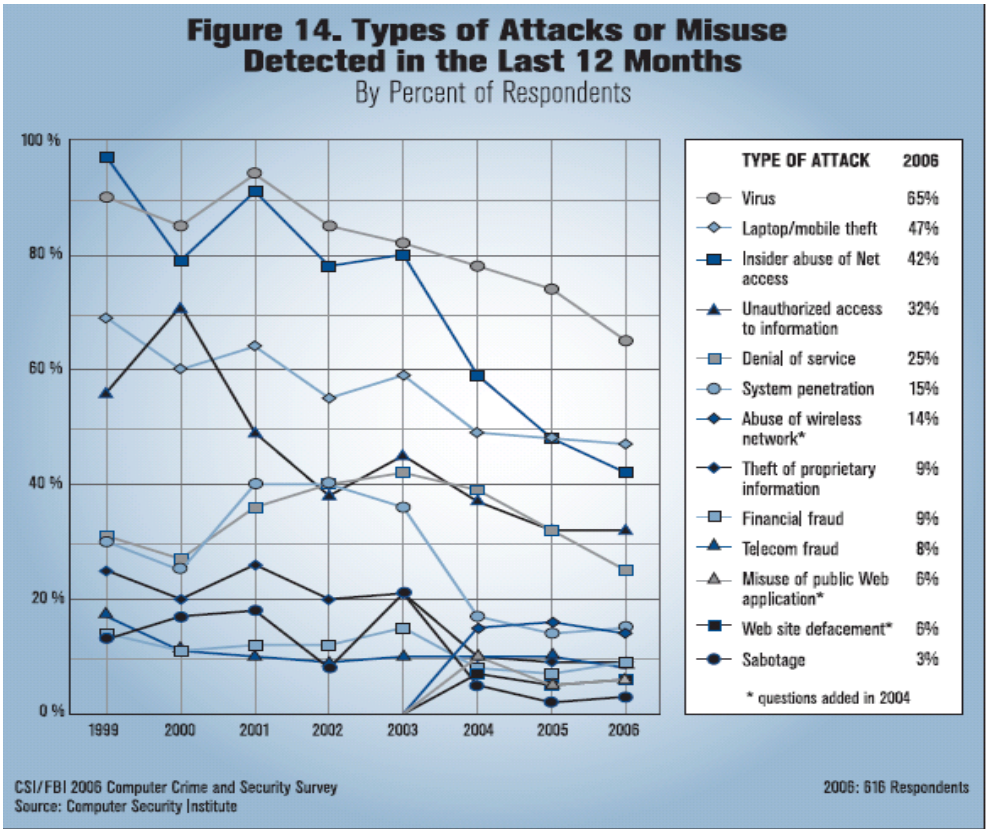
63,5% dos entrevistados adotam a ISO 27002 como a principal norma que norteia suas

empresas.
Política de segurança formalizada já é realidade em 68% das organizações.
Apenas 21% das empresas afirmaram possuir um Plano de Continuidade de Negócios (PCN) atualizado e testado.
60% das empresas fazem Planejamento de Segurança, sendo que 27% possuem planejamento para até 1 ano.
A área de tecnologia (49,5%) continua sendo a principal responsável pelo gerenciamento da segurança da informação nas empresas, seguida pela área específica, Security Office, com 25,5%.
Pelo terceiro ano consecutivo, antivírus (90%), sistemas de *backup* (76,5%) e *firewall* (75,5%) foram apontados como as três medidas de segurança mais implementadas nas empresas.
60% afirmam que os investimentos de suas empresas em segurança, para 2004, vão aumentar.
Fonte: 9ª Pesquisa nacional de segurança da informação.

Essas pesquisas demonstram o quanto é preocupante a segurança da informação, e o quanto de trabalho há pela frente para se atingir um padrão eficiente em segurança da informação.

Nesse sentido, em recente pesquisa realizada pelo CSI/FBI (2005), foi identificado que 95% das empresas pesquisadas tiveram mais de dez incidentes de segurança em seus *web sites*, e que o ataque de vírus ainda continua como a grande fonte de perdas financeiras. Nas pesquisas dos anos seguintes, o vírus ainda continuava sendo uma das principais fontes de perdas financeiras, que, juntamente com o acesso não autorizado, o roubo de *laptops* e o roubo de propriedade da informação, representam mais que 70% das perdas financeiras.

Dessa forma, reproduzimos um quadro da pesquisa realizada pelo CSI/FBI, no ano de 2006, no qual é possível identificar a liderança do ataque de vírus sobre os outros tipos de ataques, no período de 1999 a 2006. Esse quadro mostra o comportamento das principais ameaças à segurança da informação.



Na pesquisa realizada pelo AusCERT (AusCert, 2006), verifica-se que os principais tipos de ataques eletrônicos são: vírus, *worm* ou *trojan* (64%); acesso indevido à internet, *e-mail* ou recursos de sistema (62%), e roubo de *laptop* (58%), sendo o vírus e o roubo de *laptop* os maiores responsáveis pelas perdas financeiras decorrentes desses ataques.

Abaixo vem apresentado um quadro no qual constam as principais ameaças apresentadas nas 8ª e 9ª Pesquisa nacional de segurança da informação, realizadas pela Módulo Security Solutions.

Principais ameaças segundo pesquisas efetuadas pela Módulo Security Solutions

PRINCIPAIS AMEAÇAS	MODULO 2002	MODULO 2003
Funcionário insatisfeito	64%	53%
Vírus	55%	66%

Acessos locais indevidos	49%	49%
Vazamento de informações	48%	47%
Divulgação de senhas	47%	51%
Hackers	36%	39%
Uso de *notebooks*	36%	31%
Falhas na segurança física	33%	37%
Fraudes, erros e acidentes	30%	41%
TOTAL RESPODENTES	547	682

Fonte: Dantas (2011)

Pelos dados das pesquisas citadas, observa-se que, apesar da evolução da tecnologia da segurança da informação, as ameaças ainda permanecem em patamares que demandam bastante atenção, colocando sob holofotes a eficácia das medidas de proteção ao longo desse período.

Para uma melhor visualização da consolidação dessas ameaças, são apresentados, abaixo, os tipos de ameaças citadas nas pesquisas de segurança da informação.

Ameaças apresentadas nas pesquisas de segurança da informação[10]

As principais ameaças apresentadas em pesquisas de segurança da informação foram:

- ✓ Vírus, *worm,* cavalo de tróia (*trojan horse);*
- ✓ *Phishing, pharming e spyware*;
- ✓ *Adware; spam*;
- ✓ Roubo de dados confidenciais da empresa e de cliente, da propriedade da informação e da propriedade intelectual;
- ✓ Acesso não autorizado à informação;
- ✓ Perda de dados de clientes;
- ✓ Roubo de *laptop*, portáteis e de *hardware*;
- ✓ Má conduta e acesso indevido à *network* por funcionários e gerentes, bem como abuso de seus privilégios de acesso e utilização indevida da rede *wireless;*

[10] As fontes das pesquisas foram: as do CSI/FBI dos anos de 2003 a 2007; AusCERT dos anos de 2002 a 2006; as da Deloitte Touche Tohmatsu dos anos de 2005 e 2006, e da Módulo Security Solutions S.A dos anos de 2002 e 2003.

- ✓ Ataque de negação de serviço, invasão de sistemas e da network;
- ✓ Acesso e utilização indevida da internet e dos recursos dos sistemas de informação;
- ✓ Degradação da *performance*, destruição e/ou desfiguramento da *network* e do *web site*;
- ✓ *Software* de má qualidade, mal desenvolvido e sem atualização;
- ✓ Fraude financeira e de telecomunicações;
- ✓ Interceptação de telecomunicação (voz ou dados) e espionagem;
- ✓ Sabotagem de dados e da *network*;
- ✓ Desastres naturais;
- ✓ *Cyber*-terrorismo;

Das ameaças citadas nessas pesquisas, observa-se que é dispensada uma atenção especial para os *malware*[11] (códigos maliciosos). Os principais códigos maliciosos são: vírus, cavalos de tróia, *adware e spyware, backdoors, keyloggers, worms, bots e botnets e rootkits*.

O **Vírus** é um programa ou parte de um programa de computador, o qual se propaga por meio de cópias de si mesmo, infectando outros programas e arquivos de computador. O vírus depende da execução do programa ou do hospedeiro para ser ativado.

O **Cavalo de Tróia** (*trojan horse*) é um programa que executa funções maliciosas sem o conhecimento do usuário. Normalmente esse código é recebido como um presente (cartão virtual, prêmios, fotos, protetor de tela, etc.). O seu nome tem origem na mitologia grega.

O **Adware** (*Advertising software*) é um tipo de *software* projetado para apresentar propagandas, seja por meio de um navegador (*browser*), seja com algum outro programa instalado em um computador.

O **Spyware** é um *software* espião que tem como objetivo monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

Os **Backdoors** são programas que procuram dar a garantia de retorno a um computador comprometido, sem utilizar novas técnicas de invasão, ou retornarem ao computador comprometido sem serem notados.

[11] *Malware*, do inglês *malicious software* é um termo genérico usado para se referir aos programas que executam ações maliciosas.

Os **Keyloggers** são programas capazes de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

O **Worm** é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Difere do vírus por não embutir cópias de si mesmo em outros programas ou arquivos.

O **Bot** é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador. Normalmente, o *bot* se conecta a um servidor de IRC (Internet Relay Chat) e entra em um canal (sala) determinado, aguardando as instruções do invasor, monitorando as mensagens que estão sendo enviadas para esse canal. O invasor, ao se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por sequências especiais de caracteres, que são interpretadas pelo *bot*. Tais sequências de caracteres correspondem a instruções que devem ser executadas pelo *bot*.

Os **Botnets** são as redes formadas por computadores infectados com *bots*. Essas redes podem ser compostas por centenas ou milhares de computadores. Um invasor que tenha controle sobre uma *botnet* pode utilizá-la para aumentar a potência de seus ataques, por exemplo: para enviar centenas de milhares de *e-mails* de *phishing* ou *spam*; para desferir ataques de negação de serviço, etc.

O **Rootkits** é um conjunto de programas que utiliza mecanismos para esconder e assegurar a presença do invasor no computador comprometido.

Como muitas das ameaças à segurança da informação vêm do ciberespaço, pode ser que haja uma tendência para se dispensar uma atenção maior ao tratamento dessas ameaças, o que pode tornar essa avaliação vulnerável. Por exemplo, **Kevin Mitnick,** um ex-*hacker*, em seu livro "A Arte de enganar", deixa bastante claro que muito de seus ataques de sucesso sequer utilizavam ferramentas para a invasão de sistemas: bastava uma boa conversa e a exploração de falhas no controle de acesso físico.

Como já foi abordado, para que as ameaças possam ser identificadas faz-se necessário recorrer às pesquisas de segurança da informação. Contudo, elas por si só não são suficientes para uma delimitação das principais ameaças, uma vez que essas pesquisas dão ênfase maior às ameaças do meio

eletrônico. As ameaças como fogo, inundação, tempestade, descargas elétricas, bem como as ações violentas de pessoas de fora das organizações, como: incêndios criminosos, ataques de bombas e vandalismo, devem, também, integrar esse grupo nas suas avaliações.

Dessa forma, sempre que se for avaliar uma ameaça, deve-se identificar não apenas o que é oriundo do meio eletrônico, como as da classe dos códigos maliciosos, mas também outros tipos de ameaças que não utilizam esse meio.

Nesse sentido, a BS 7799-3:2006, em seu anexo "C", e o HB 231:2004, em seu anexo "A", fornecem uma lista de ameaças à segurança da informação, e dentre elas encontram-se ameaças que não são exclusivas ao meio eletrônico, como, por exemplo: atos de terrorismo, falta ou carência de sistemas de refrigeração, brechas na legislação, danos causados por funcionários e por terceira parte, desastres naturais, fogo, acesso não autorizado às instalações, etc.

Ao se avaliarem as ameaças à informação, devem-se considerar as vulnerabilidades possíveis e existentes, bem como as possibilidades de concretização dessas ameaças. Neste processo de análise, adentra-se no estudo do risco ao se procurar entender como essas ameaças ocorrem e qual a sua relação com as vulnerabilidades, como também a probabilidade de sua concretização, para que seja possível efetuar um tratamento mais adequado aos riscos, de acordo com as reais condições da organização.

2. ASPECTOS PRELIMINARES AO ESTUDO DO RISCO

Em um cenário de incertezas, as ameaças e oportunidades têm o potencial de produzir perdas ou aumentar os ganhos. Os resultados positivos são alcançados com uma boa gestão das incertezas e de seus riscos, gerando valor ao otimizar as suas oportunidades, e ao estabelecerem estratégias para os objetivos de crescimento, na busca da maximização de seus resultados. Os resultados negativos são oriundos da ausência e/ou da fragilidade dessa gestão, em que os seus resultados podem produzir danos e perdas de grandes proporções.

Como já foi visto, várias são as ameaças aos negócios corporativos, e em especial à informação e aos seus ativos. Os dados apontados nas pesquisas de segurança da informação demonstram o tamanho do problema para as organizações com relação aos riscos, e a magnitude do desafio da eliminação e controle sobre eles.

Nesse cenário, o estudo do risco assume um importante papel nas corporações do mundo moderno ao proporcionar-lhes um processo de gerenciamento baseado nos riscos.

O ponto de partida para se iniciar o estudo do risco é o de se poder entender o que é um risco. Para isso, torna-se necessário apresentar um conceito claro do que seja o risco.

2.1 Conceito do risco

O risco é compreendido como algo que cria oportunidades ou produz perdas. Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas.

Vários conceitos e definições podem ser encontrados para a definição do risco; contudo, o conceito adotado, neste livro, para o risco é aquele estabelecido pela norma ISO/IEC Guide 73:2002,[12] que define o risco[13] como:

[12] Essa norma apresenta as terminologias a serem utilizadas no gerenciamento de riscos e uma abordagem na descrição dessas atividades.

"A combinação da probabilidade[14] de um evento[15] e suas consequências."[16]

Abaixo, são apresentados outros conceitos de risco:

A norma AS/NZS 4360:2004[17] define risco como a oportunidade de acontecimento de alguma coisa que causará impacto nos objetivos. Para essa norma, o risco é geralmente especificado em termos de um evento e/ou circunstâncias e suas consequências, e é medido pela combinação das consequências de um evento e sua probabilidade. Ele pode ter um impacto positivo ou negativo.

O HB 231:2004[18] refere-se ao risco como sendo a chance de alguma coisa acontecer, que deverá produzir um impacto sobre os objetivos, o qual é medido em termos da probabilidade e consequências.

Brasiliano (1999:103) define a ameaça ou risco na segurança empresarial como sendo um evento capaz de produzir perdas reais e mensuráveis por um padrão comum. Para esse autor, o risco pode ser definido como uma ou mais condições de variáveis com um potencial necessário de causar dano ao patrimônio da empresa, seja ele tangível, seja intangível.

O Guia de Gerenciamento de riscos (Microsoft, 2005) estabelece que o risco está relacionado com a probabilidade de ocorrência de um evento que afete os negócios.

Pode-se concluir, portanto, que o risco está relacionado com a probabilidade de um evento e suas consequências.

Dessa forma, toda vez que nos referirmos ao termo risco, deveremos sempre atentar para a probabilidade de concretização de um evento e suas consequências. E essas consequências são as negativas.

---

[13] Os termos e definições empregados neste livro estarão alinhados ao padrão das normas internacionais ISO e AS/NZS.

[14] A probabilidade associada a um evento é calculada para determinado período de tempo, e é definida como um número real na escala de 0 a 1 associado a um evento aleatório, que pode estar relacionado a uma frequência de ocorrência relativa de longo prazo ou a um grau de confiança de que um evento irá ocorrer. Para um alto grau de confiança, a probabilidade está próxima de 1.

[15] Por evento deve ser entendida a ocorrência de um conjunto particular de circunstâncias, que pode ser uma única ocorrência ou uma série delas. A probabilidade associada a um evento pode ser estimada em um dado período de tempo.

[16] Por consequência, deve ser entendido o resultado de um evento.

[17] Essa norma fornece um guia genérico para o gerenciamento de riscos.

[18] Essa norma fornece um guia para o gerenciamento de riscos de segurança da informação.

Equação do risco

Como anteriormente foi definido, o risco é representado pela combinação de dois elementos: a consequência e a probabilidade. E essas variáveis podem ser representadas por uma equação.

Casada et alli (2003) apresenta uma equação para o risco, representando-o como o produto da frequência (quantidade de eventos em determinado período) pela consequência ou impacto do evento.

R= C x **P**

R = risco; **C =** consequência; e **P=** frequência

Geralmente, a frequência é estimada em dados históricos ou calculada com base na possibilidade de combinação de eventos externos, erros humanos e falhas de equipamentos e sistemas que mais contribuem para a ocorrência do risco.

Para a utilização de dados históricos, deve-se atentar para o registro de eventos nas organizações. Geralmente, não é consistente. Uma opção é o levantamento desses dados tendo como base as pesquisas sobre segurança da informação, para que seja possível obter maior confiabilidade.

Já para o cálculo baseado na combinação de eventos externos utiliza a combinação da ameaça com a vulnerabilidade, podendo vir a ser representado por **P= T** x **V**, em que: **T=** ameaça; e **V=** vulnerabilidade**.**

A consequência é expressa pela soma dos efeitos possíveis de um ataque (ocorrência de um evento) a um determinado cenário. Pode incluir a soma de várias categorias de cenários. O somatório dessas consequências deve anexar os efeitos intangíveis, como o capital intelectual e o impacto na sensação de segurança. Essas consequências podem ser delimitadas por valores financeiros e por níveis.

O manual de gerenciamento de riscos (HB 436:2004) segue essa mesma linha de raciocínio ao expressar o risco em função da consequência e probabilidade, e apresenta a seguinte equação:

R= C x L, em que **R =** risco; **C =** consequência; e **L=** probabilidade

Sêmola (2003) apresenta a seguinte equação para o risco, diferenciando-se por acrescentar as medidas de segurança, que, segundo ele, devem ser consideradas na aferição do risco:

R= (V x **A** x **I)/M**, em que

V= vulnerabilidade; **A**=ameaça; **I**=impacto; e **M**=medidas de segurança.

Vários fatores influenciam na medição do risco, e dentre eles devem ser considerados os controles ou as medidas de segurança, que interferem diretamente na redução ou no aumento do risco.

Um outro elemento para essa aferição é a utilização de um fator de peso, por meio de uma operação exponencial, como está citado em HB 436:2004, que apresenta a seguinte equação empregando um fator de peso: $\mathbf{R} = (\mathbf{C} \times \text{Fator de peso})^{x} \times (\mathbf{L})^{y}$.

O emprego da equação do risco para uma aferição exata não é simples, e a sua grande dificuldade consiste na relação com a aferição de suas variáveis: consequência e probabilidade. Primeiro, porque entendemos ser bastante difícil a sua valoração, principalmente ao se calcular o dano à imagem da empresa ou à marca de um produto (intangível). Segundo, pelo fato da baixa confiabilidade dos dados estatísticos nas organizações, e também pelo fato de a metodologia empregada nas pesquisas poder não representar a realidade da organização a ser avaliada.

Contudo, o que é importante ao utilizar a equação do risco, é poder compreendê-lo de uma maneira mais ampla, dando transparência aos elementos que influenciam na sua identificação, para uma melhor análise.

Outro aspecto que deve ser observado no estudo do risco é a possibilidade de se identificar a sua origem, o que torna possível classificá-lo em categorias.

2.2 Origem e classificação dos riscos

O risco pode ter várias origens, pode ser oriundo de eventos da natureza, pode ser decorrente de problemas técnicos, bem como ser o resultado de uma ação intencional. Entender a sua origem e estabelecer uma classificação é um ponto facilitador para se compreender o risco.

Os riscos podem ser classificados em várias categorias, como, por exemplo: incontroláveis, técnicos, de mercado, de crédito, operacionais, legais, humanos. Classificar os riscos em categorias objetiva segregá-los para que seja possível dar-lhes uma melhor visibilidade, dispensando-lhes um tratamento mais específico.

A opção que apresentamos para a classificação do risco é feita com base na origem das ameaças e vulnerabilidades. Dessa forma, classificamos os riscos em 3 categorias: os naturais, os involuntários e os intencionais.

Os riscos classificados como **naturais** são aqueles oriundos de fenômenos da natureza; os **involuntários** resultam de ações não intencionais, relacionados com vulnerabilidades humanas, físicas, de *hardware*, de *software*, dos meios de armazenamento e das comunicações; e os **intencionais** são aqueles derivados de ações deliberadas para causarem danos, e têm sua origem no ser humano.

Estabelecidas essas categorias, a etapa seguinte é identificar os principais fatores que possam motivar o risco, pois sabemos que a concretização de um evento pode ser independente da intenção do agente ou do nível de controle existente, como os eventos da natureza, por exemplo.

O que se pretende alcançar é estabelecer um nexo de causalidade entre os eventos e os fatores condicionantes existentes na organização, que poderão concorrer para a concretização de um risco.

Um aspecto que merece reflexão é como trabalhar a definição do risco, relacionando a sua origem com possíveis condições que permitam motivá-lo, para que seja possível entender o que é um risco. Muitas vezes, não se consegue desenvolver uma cultura voltada para os cuidados com os riscos, por não se compreender o que ele representa, bem como o poder que ele tem de produzir resultados negativos.

Verifica-se, em muitas organizações, que o trato com os riscos é bastante limitado em se referindo ao envolvimento com os funcionários. Essa falta de clareza é transformada em obstáculo ao sucesso do gerenciamento de riscos.

Objetivando superar essa barreira, o caminho que entendemos ser o mais adequado é o de apresentar um conceito internacionalmente aceito para o risco, e então classificá-lo de acordo com a origem das vulnerabilidades e ameaças. Dessa forma, ao serem apresentados os principais riscos que afetam a segurança da informação, e ao serem apontados os possíveis fatores que possam motivá-los, não apenas se estará trabalhando a percepção das pessoas para uma atenção maior para com os riscos, como também se estará proporcionando o entendimento do risco e semeando uma cultura da segurança da informação.

Considerando o objetivo didático deste livro, apresentamos, a seguir, alguns fatores motivadores por categorias de risco.

Riscos naturais

Para os riscos naturais, dependendo do potencial do evento, pode parecer difícil haver uma proteção eficaz, mas, sabendo-se que tais eventos são comuns em determinada região, torna-se mais fácil adotar ações planejadas para prevenir os impactos, minimizar os danos quando de sua concretização, e poder retornar à normalidade das atividades.

Abaixo apresentamos alguns fatores que devem ser considerados com relação a essa categoria de risco:

1- A área em que a empresa está instalada é sujeita a eventos da natureza, constantes ou não, de proporções catastróficas ou não;
2- Falta de acompanhamento de boletins meteorológicos;
3- Material empregado na construção de baixa resistência e/ou qualidade.
4- Equipamentos de prevenção a sinistros (de origem na natureza) sem inspeção periódica e de má qualidade;
5- Ausência de plano de recuperação de desastres e de continuidade dos negócios;
6- Falta de treinamento em ações contingenciais.

Riscos involuntários

Para os riscos involuntários, a identificação da sua origem tem relação direta com as vulnerabilidades humanas, físicas, de *hardware*, de *software*, com os meios de armazenamento e as comunicações, e que geralmente ocorrem por falha na condução do sistema de gerenciamento de segurança da informação. Contudo, alguns fatores devem ser considerados com relação aos riscos involuntários, tais como:

1- Falha nos equipamentos de prevenção e detecção;
2- Descuido no cumprimento de normas para guarda, transporte e manuseio de material inflamável;
3- Material de fácil combustão empregado na construção;
4- Equipamentos ligados 24 horas;
5- Ausência de treinamento em medidas contingenciais;
6- Inexistência de processos de qualidade;

7- Inexistência de controles internos;
8- Inexistência de programa de capacitação continuada;
9- Cultura organizacional.

Riscos intencionais

Já para os riscos intencionais, geralmente os fatores motivadores estão diretamente relacionados com o tipo de negócio, tipo de produto, tipo de mercado, localização geográfica, com o sistema de controle interno e o nível de segurança existente.

Ele ocorre pela exploração intencional de um agente (interno ou externo) ao perceber alguma falha no sistema de proteção da empresa, ou ao executar ataques diretos ou aleatórios, com o objetivo de detectar alguma vulnerabilidade nesse sistema.

Observe-se que, além de se identificar a origem do risco, nessa categoria, deve-se, também, identificar o porquê da ação de pessoas, o motivo delas, sejam quais forem os seus interesses, para atentarem contra uma instituição ou pessoas. O foco dessa análise está na identificação dos principais pressupostos do agente causador do dano. Trata-se de identificar quais os pressupostos que podem levar uma pessoa a cometer uma ação deliberada contra a organização.

Essa análise pontual está relacionada com a percepção dos diretores, funcionários, membros da equipe de gerenciamento de riscos, pessoas da organização em geral, colaboradores (consultor em segurança, auditor, etc.), na tentativa de compreender que determinado ativo da organização desperta interesse em terceiros, e que, por emio de uma ação oportuna e intencional, eles podem tentar provocar algum dano.

Por exemplo, é realizar uma análise sobre os motivos que podem levar um funcionário a utilizar indevidamente um sistema. Não é a análise sobre a violação dos requisitos de proteção do sistema, mas sim, saber identificar o que motivou aquele funcionário a cometer determinada ação contra a empresa, um produto, um processo, etc.

Alguns fatores devem ser considerados com relação aos riscos intencionais, tais como:

1- Situação do sistema de controle interno;
2- Atratividade do produto e sua fácil receptação no mercado paralelo;

3- Área em que a empresa está instalada sujeita a eventos da natureza de proporções catastróficas;
4- Situação da criminalidade na região em que a empresa está instalada;
5- Sensação de impunidade;
6- Pagamento efetuado, em espécie, aos funcionários da empresa;
7- Funcionários insatisfeitos com salários em atraso e sem perspectiva de continuidade no emprego;
8- Mercado altamente competitivo;
9- Informações de alto poder estratégico.

Observe-se a importância dessa percepção, uma vez que ela é uma peça importante dentro do contexto de uma abordagem mais ampla no estudo dos riscos. Essa percepção, além de estar relacionada com a origem do risco, abrange, também, o que para a empresa poderá motivar a sua ocorrência.

A concretização de um risco pode estar associada a mais de um evento, como a concorrência de mais de uma categoria. Por exemplo, citamos a ocorrência de um incêndio decorrente da queda de um raio (evento natural), quando o para-raios e os sensores de incêndio não funcionaram, o pessoal de combate ao fogo não acionou a unidade dos bombeiros, nem agiu de acordo com o estabelecido no plano de contingências, tendo a empresa perdido todo o seu banco de dados, sem oportunidade de recuperá-lo por não possuir um procedimento para *backup*.

No exemplo acima, encontramos a concorrência concomitante de mais de uma vulnerabilidade para a concretização do risco (queda de um raio): a humana (não cumprimento dos planos e procedimentos), a técnica (falha dos sensores e do para-raios) e a organizacional (sem plano de contingência). Nesse exemplo, o risco é classificado na categoria dos riscos naturais, por ter sido um evento da natureza a origem causadora dos danos.

Note-se que tal classificação facilita a compreensão do risco, uma vez que fica mais clara a sua identificação, tornando mais direta a compreensão do risco e o estabelecimento de ações para o seu tratamento.

E é justamente essa capacidade de percepção e de entender os negócios, missão e ativos corporativos, que tornará o processo de gerenciamento de riscos mais eficiente e eficaz.

2.3 O ambiente e as atividades de negócios

A compreensão do ambiente e das atividades de negócios é outro ponto fundamental no estudo do risco, uma vez que a profundidade da análise estará diretamente relacionada com essas duas variáveis.

As informações básicas para se compreender o ambiente de negócios estão no planejamento estratégico da organização, que é o documento no qual deverá constar uma análise do cenário da organização. Caso a empresa não possua essas informações disponibilizadas no seu planejamento estratégico, ou o cenário não esteja claro, deverão ser considerados os seguintes aspectos para se compreender o ambiente de negócios: a noção SWOT, a projeção e a prospecção.

Noção SWOT

A noção de *SWOT* é uma técnica de construção de cenário que foi introduzida pela ***Escola de estratégia do Design***, ao propor um modelo de formulação de estratégia que busca atingir uma adequação entre as capacidades internas e as possibilidades externas (Mintzberg, Ahlstrand e Lampel, 2000). Essa técnica proporciona a avaliação dos pontos fortes (*Strenghts*) e dos pontos fracos (*Weaknesses*) da organização à luz das oportunidades (*Opportunities*) e das ameaças (*Threats*) em seu ambiente.

As forças são situações positivas que existem instaladas no ambiente interno da organização, as quais favorecem o desenvolvimento das atividades empresariais, gerenciais e operacionais. As fraquezas são situações negativas que existem instaladas no ambiente interno da organização, as quais atrapalham e dificultam o desenvolvimento das atividades empresariais, gerenciais e operacionais.

As oportunidades são situações de potencialidades que existem no ambiente externo da organização, as quais podem e devem ser aproveitadas para viabilizar o alcance dos objetivos e metas da organização. As ameaças são situações de vulnerabilidade que existem no ambiente externo da organização, as quais podem comprometer e inviabilizar o alcance dos objetivos e metas da organização.

Essas quatro variáveis formam um cenário bastante utilizado para se compreender o ambiente organizacional, tanto interno quanto externo. Contudo, a compreensão do cenário não deve ser limitada ao emprego da noção SWOT, pois ao final dessa análise tem-se uma fotografia da situação, que é estática, e como sabemos, o ambiente é mutável e oscila de acordo com variáveis que surgem a cada dia.

Um problema encontrado com o emprego da noção SWOT é que não são feitas as inter-relações das variáveis encontradas, constituindo-se numa abordagem textual e desassociada das outras variáveis, resumindo-se a apenas identificar pontos isolados. E esse problema é típico do emprego da noção SWOT.

Para que esse problema seja corrigido, é necessário realizar uma associação das variáveis, para que haja uma correlação entre elas, ou seja, dos fatores externos com os internos. Dessa forma, poderão ser identificados quais os fatores externos que atuam ou influenciam os negócios e provocam oportunidades e ameaças, quais as oportunidades e ameaças que estão presentes, e ainda aquelas que não estão, mas que podem ser vislumbradas como uma possível ameaça, e como a organização se apresenta para enfrentar cada oportunidade e ameaça.

Projeção

A projeção é realizada com base em acontecimentos passados e é bastante utilizada com base na avaliação das estratégias de períodos anteriores. Geralmente são projetados três cenários: um menos otimista, um normal, e um mais otimista. Ela é feita após a análise das informações, por ocasião do emprego da noção SWOT.

Prospecção

A prospecção é uma técnica de elaboração de cenários que tem como objetivo estudar as diversas possibilidades de futuros plausíveis existentes e preparar as organizações para enfrentarem qualquer uma delas, ou até mesmo criar condições para que modifiquem suas possibilidades de ocorrência ou minimizarem seus efeitos. É um estudo do futuro.

Essa técnica vem sendo utilizada com o objetivo de minimizar riscos e permitir a manutenção do posicionamento competitivo da organização no mercado. Tem como fundamento básico que o futuro é múltiplo e incerto.

Essa técnica estuda os fatos portadores de futuro e tem como base os pontos fortes e fracos e as oportunidades e ameaças, a técnica do *Brainstorming* aplicado às diversas áreas da empresa, e a opinião dos especialistas durante a leitura dos fatos passados e presentes. Não é uma técnica de fácil emprego, mas aumenta as chances da organização fazer uma leitura focada em futuros possíveis e plausíveis, o que lhe possibilitará condições de antecipação para conduzir uma mudança de rumo, caso ocorra um movimento de ruptura de tendência.

Para a comunidade da segurança, de uma maneira geral, saber tratar com possibilidades futuras é um grande desafio e diferencial no sucesso com as incertezas dos eventos imprevisíveis, pois sabemos que, ao trabalharmos com planos de continuidade, estaremos tratando de possibilidades de: se tal evento acontecer, o que deveremos fazer. Em outras palavras, são possibilidades baseadas em estudos de situações passadas, em dados estatísticos de ocorrências passadas e em possíveis fatos portadores de futuro, e tudo isso alinhado ao planejamento estratégico da organização.

E justamente para atender a essa filosofia de visão é que a comunidade da segurança da informação deve cada vez mais estar alinhada com os propósitos organizacionais e entender o contexto geral do ambiente de negócios das corporações, para poder oferecer serviços cada vez mais especializados e necessários.

Atividades de negócios

Outra questão importante é compreender as atividades desenvolvidas pela organização, pois, dependendo da atividade, o risco pode ser constante, demandando uma avaliação mais detalhada a identificação dos tipos de ameaças e as possibilidades de quebra de controles pela investigação de vulnerabilidades em sistemas e equipamentos, inclusive com a utilização de alta tecnologia. Tudo isso se deve ao fato da importância e da criticidade da informação e dos ativos em questão.

Para demonstrar a relevância desse assunto, tomaremos como exemplo uma experiência realizada para identificar vulnerabilidades em

sistemas de controle de acesso. Esse estudo foi apresentado na Universidade de *Yokohama* e versa sobre os sistemas de controle de acesso baseados na identificação biométrica de digitais, o qual demonstrou que tais sistemas podem ser fraudados com a utilização de uma digital artificial construída com material gelatinoso (Matsumoto, 2004).

Nesse estudo, foi demonstrado que várias ações podem ser realizadas para fraudar sistemas de identificação por digitais, inclusive utilizando um molde em gelatina, que é facilmente elaborado e sem grandes recursos tecnológicos.

Outro exemplo decorre das experiências realizadas para a captura de dados utilizando equipamentos à distância, o que demonstra vulnerabilidades em equipamentos que utilizam LEDs (Light Emitting Diode) como *modems*, roteadores e monitores. Numa delas, Loughry e Umphress (2002), pesquisadores da Universidade de Auburn, provaram que a utilização de um telescópio poderia capturar os dados a uma distância considerável pela simples visualização desses sinais luminosos. Em outra experiência, Kuhn (2002), da University of Cambridge, demonstrou que dados poderiam ser capturados com o emprego de fotossensores para ler os sinais do *display* à distância. Neste último, foi utilizado um equipamento para ler os sinais do CRT (Cathode-ray tube) pela intensidade da luz emitida. Em ambos os casos, ficou demonstrada a vulnerabilidade dos equipamentos que utilizam esses dispositivos.

Em recente estudo, pesquisadores da Princeton University (New Jersey, USA) desenvolveram uma pesquisa[19] que aplicou um método para capturar dados criptografados armazenados no disco rígido de um computador, com a simples técnica de aplicar um jato de ar frio de um spray removedor de poeira. Com isso, eles mostraram que os dados criptografados podem ser vulneráveis a essa técnica, devido a uma fragilidade pouco conhecida dos *chips* de memória dinâmica de acesso aleatório. Essa técnica de roubo de informações pode ser utilizada para a captura de dados criptografados em computadores portáteis, que são alvos de constantes roubos.

[19] Lest We Remember: Cold Boot Attacks on Encryption Keys. disponível em:<http://citp.princeton.edu.nyud.net/pub/coldboot.pdf>

Os exemplos acima demonstram que até tecnologias tidas como avançadas são susceptíveis às vulnerabilidades, como também que os mais rigorosos controles de acesso podem ser violados, à distância, em tecnologias reconhecidas como seguras.

Ao se trazerem essas experiências para a realidade, pode-se ter a certeza de que a utilização desses dispositivos para a quebra de controles seria motivada pela importância das informações processadas e do tipo de negócio realizado, dentro de um contexto altamente competitivo. É nesse sentido que a comunidade de segurança da informação deve alinhar o estudo sobre os riscos, considerando como aspectos fundamentais a compreensão do ambiente e as atividades de negócios, para que a sua gestão sobre riscos não seja vulnerável e comprometa o sucesso dos negócios.

2.4 Prevenção X Reação

Quando se trata de segurança, dois aspectos devem ser levados em consideração no estudo do risco: a prevenção e a reação.

É mister saber que, até o momento do evento, as ações de gerenciamento dos controles dos riscos constituem todo um conjunto de ações a serem empregadas no dia a dia, e que, se de alguma forma forem insuficientes para evitar um ataque, terão como complementos ações outras que objetivam fazer com que a organização retorne ao *status quo* anterior ao momento da concretização do risco.

Justamente por olhar sob esse prisma é que entendemos que o estudo do risco deve ser direcionado para esses dois tipos de situação: prevenção e reação. A prevenção engloba o conjunto de ações que objetiva evitar e detectar a possibilidade de eventos danosos aos negócios corporativos. A reação é caracterizada pelas ações de resposta e diz respeito à adoção de medidas a partir da ocorrência de um evento. Objetiva não só o retorno à normalidade das atividades como também a minimização dos impactos causados.

A sua grande diferença está no aspecto temporal: a prevenção, na antecipação, detecção, tratamento e aceitação de riscos, e a reação, no momento da resposta a ações posteriores. Em outras palavras, essas duas

abordagens devem alcançar três fases: antes, durante e após um evento, ou seja, antes, a prevenção, e, durante e após, a reação.

Ambas as abordagens, mesmo que possuam ações com focos temporais diferentes têm como características comuns: serem estruturadas em um mesmo estudo do risco e convergirem para um mesmo objetivo geral, que é o de manter a normalidade das atividades de negócios.

Geralmente essas ações são consolidadas em planos de continuidade de negócios (*Business Continuity Plan* - BCP) e de recuperação de desastres (*Disaster Recovery Plan*- DRP).[20]

Atenção específica deve ser dispensada a esses instrumentos que fazem parte de um conceito maior de prevenção, que é o de se antecipar o imprevisível, ao se estabelecer uma gestão voltada para a continuidade dos negócios, em que as ações de prevenção, resposta e recuperação da concretização dos riscos são criteriosamente planejadas, o que cria um ambiente mais competitivo.

Além de otimizar o tempo para as atividades mais importantes da organização, esse processo (gerenciamento da continuidade dos negócios) evita o desperdício de recursos e o seu aporte indevido para uma reação a um evento danoso.

Mesmo quando se considera que as ações de resposta e recuperação fazem parte do conceito de reação, tudo isso é alcançado pela amplitude da filosofia da prevenção, ao se estabelecer um planejamento para esses momentos de crise. Com isso chamamos a atenção específica para aquelas organizações nas quais as ações de prevenção e reação são limitadas ao emprego de ferramentas, ações e processos fragilizados, não sendo sustentadas por um estudo do risco.

Dessa forma, ratifica-se que o estudo do risco deve estar voltado para duas situações: uma é a antecipação de eventos que podem vir a comprometer os negócios corporativos, e outra durante e após a ocorrência desses eventos.

[20] Uma variedade de termos pode ser encontrada quando nos referimos à continuidade de negócios e à recuperação de desastres, tais como: gerenciamento de emergências, gerenciamento de crise, gerenciamento de incidente, plano de contingência. Têm-se utilizado esses termos de forma indiscriminada, servindo tanto para a prevenção, quanto para a reação.

2.5 Métodos de análise e parâmetros de avaliação

Como já foi visto, o risco é medido pela probabilidade e suas consequências, e o seu estudo deve estar voltado tanto para a prevenção como para a reação. Nesse estudo dois aspectos merecem especial destaque quando analisamos e avaliamos o risco. Um tem relação ao método escolhido para estimar a probabilidade e aferir a consequência de um risco, e o outro diz respeito aos critérios de escolha para a parametrização da criticidade do risco.

A escolha do método deve ser realizada sob 2 prismas: o qualitativo e o quantitativo. A análise qualitativa é geralmente utilizada quando não existe a disponibilidade de dados, ou quando eles são precários, e a sua análise é realizada com base em valores referenciais. A análise quantitativa é utilizada quando os dados são confiáveis e estão disponíveis, e a sua análise é realizada com base em valores absolutos.

Existem ocasiões em que o método qualitativo é mais apropriado, como no caso de reuniões para a conscientização da importância de se atentar para determinado tipo de risco, ou quando não for necessário um detalhamento maior da análise. Já o método quantitativo apresenta-se mais apropriado quando é utilizado para mensurar o custo monetário do risco e relacioná-lo com as medidas de proteção a serem adotadas, e quando forem analisados riscos de grandes impactos.

Método quantitativo

O método quantitativo de análise de riscos é utilizado quando a probabilidade de um evento pode ser medida em valores numéricos, e a sua consequência pode ser calculada em perdas financeiras. É o método que apresenta o custo monetário do risco.

Utiliza-se esse método quando a organização possui registros de eventos ocorridos, pois não se deve utilizar esse método sem a disponibilidade de dados, e que eles sejam confiáveis.

Partindo do pressuposto de que os dados são confiáveis, o risco pode ser calculado com base na frequência, na média, no seu desvio padrão e no coeficiente de variação, para se poder confrontá-lo com a consequência, estabelecendo o impacto e severidade do risco para cada cenário.

Cálculo da possibilidade

A possibilidade ou **probabilidade de um evento P(E)** é um valor hipotético, fixo, decorrente de uma tendência à estabilização de uma frequência relativa, à medida que cresce o número de repetições do experimento.

$$P(E) = \lim_{n \to \infty} \frac{f_E}{n}$$

P(E) = probabilidade de ocorrência do evento E
f_E = frequência absoluta do evento E
n = tamanho da amostra ou número de repetições do experimento

A sua precisão está relacionada com a quantidade de dados disponíveis sobre determinado risco, pois trabalha-se com o número total de eventos e o número de vezes que o evento ocorreu. É lógico que a concretização de um risco envolve vários fatores, que devem ser estudados em conjunto com a frequência de tais eventos.

Outro emprego desse método dá-se com a **média aritmética ($\bar{x}$)**. Essa medida de posição nos dará a frequência dos diversos valores existentes da variável.

Sendo $x_i\,(i = 1,2,....,n)$ o conjunto de dados, definimos sua média aritmética por:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n}$$

A média precisa ser complementada pelas medidas de dispersão, que caracterizam o nível de variação do conjunto de eventos. As medidas a serem utilizadas são o desvio padrão e o coeficiente de variação.

O **desvio padrão (s)** é calculado pela raiz quadrada positiva da variância, que é a média dos quadrados das diferenças dos valores em relação à sua média.

$$s_x = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n}}$$

O **coeficiente de variação (cv)** é definido pelo quociente entre o desvio padrão e a média. Ele indica a probabilidade de o resultado se manter ou não, e é frequentemente medido em percentagem. A sua vantagem é caracterizar a dispersão dos dados em termos relativos ao seu valor médio.

Nos estudos de riscos por esse método, recomenda-se que seja sempre considerado o seu coeficiente de variação, a fim de que enganos de interpretação desse tipo sejam evitados, proporcionando uma avaliação mais precisa.

$$cv(x) = \frac{s(x)}{\bar{x}}$$

Exemplificando: Uma empresa registrou no último quadrimestre vários ataques de negação de serviço, os quais deixaram os sistemas indisponíveis, gerando prejuízo de U$ 10.000, em cada ataque.

Os registros estavam assim distribuídos: 4 ataques em janeiro, 5 em fevereiro, 3 em março e 2 em abril.

A média de ataques por mês foi de 3,5 ataques, ou seja, o total de eventos (4+5+3+2=14) dividido pelo período (quatro meses), para representar a média de ataques por mês. O desvio padrão calculado foi de 1,29 e o seu coeficiente de variação foi de 37%, ou seja, o resultado apresentou uma estimativa de 37% de diferir da média, e uma estimativa de 63% de manter a média. Esse cálculo irá ser muito útil na estimativa da perda esperada.

Como pode ser verificado, a utilização desse método para o estabelecimento da probabilidade de um evento acontecer requer o conhecimento da estatística e de um registro de dados confiáveis, para que não sejam estabelecidos parâmetros aquém da real possibilidade.

Cálculo da consequência

Avaliar a consequência é estabelecer o impacto negativo da ocorrência de um evento, e é realizada por meio do cálculo financeiro dos

danos possíveis aos negócios e ativos. Esse cálculo é geralmente realizado com o cálculo do custo para a reposição do ativo e da perda esperada.

O cálculo da reposição do ativo pode ser feito no valor de mercado, isto é, o *quantum* que a empresa iria gastar para adquirir um novo ativo.[21] Esse cálculo poderá incluir ainda todas as despesas envolvidas na substituição do ativo, como transporte, alocação de mão de obra para o exame do ativo adquirido e seus ajustes para funcionamento, treinamento do usuário e pessoal de suporte, etc.

Outra forma de se calcular é com base no retorno do investimento que o valor utilizado para repor o ativo proporcionaria à organização, se aplicado no mercado financeiro e em coligadas e controladas, ou no custo da captação de recursos para a nova aquisição do ativo quando financiado. Observe-se que a taxa de aplicação normalmente é menor do que a taxa de captação.

A perda esperada é calculada no *quantum* a empresa perderá se determinado evento vier a se concretizar. A perda pode ser calculada apenas para a expectativa de receita de vendas, como também pela estimativa do impacto na imagem da empresa e nos valores das ações.

Deve ser observado que a indisponibilidade de serviços para o cliente sempre abala a sua confiança na qualidade dos serviços, devendo, também ser mensuradas.

Exemplificando: No exemplo anterior, o número médio de eventos foi de 3,5, com uma probabilidade de 63% da média de ataques se manter. Se for considerado que cada ataque gerou uma perda de U$ 10.000, o cálculo da perda esperada será feito aplicando-se o percentual de 63% sobre 10.000, que é o valor de perda por ataque, o que resulta numa perda de U$ 6.300 por evento, que multiplicado pela média de eventos, dará uma expectativa de perda total de U$ 22.050.

Aspectos que devem ser considerados quando do emprego desse método
Cálculo do valor de ativos

Determinar um valor para um ativo tangível não é difícil, pois poderá ser feito com base no seu custo de aquisição ou no custo para a sua reposição,

[21] É importante ressaltar que o valor de reposição é diferente do valor do ativo constante dos relatórios contábeis, valor que, nesses relatórios, é registrado pelo custo de aquisição e suas depreciações, diferentemente do valor de mercado de um novo ativo.

que no caso seria o valor de mercado mais as despesas operacionais. Já para se atribuir um valor para ativos intangíveis é mais difícil, pois nem sempre essa mensuração corresponde ao verdadeiro valor desse intangível.

Como exemplo, o valor de um ativo pode ser calculado: pelo seu valor para a organização; pelo impacto financeiro imediato da perda do ativo; e pelo impacto indireto causado aos negócios da corporação.

Cálculo do custo dos controles e retorno sobre o investimento

Determinar o custo dos controles é apropriar os gastos a todo e qualquer evento relacionado com o controle, a saber, todos os custos associados a aquisição, teste, implementação, operação e manutenção de cada controle. Entra nesse cálculo o valor gasto nas auditorias, consultorias, etc.

O retorno sobre o investimento pode ser calculado com base na redução das perdas esperadas (perdas antes – perdas após), deduzido o custo anual dos controles. Outra forma de se efetuar esse cálculo é pela medição do retorno financeiro sobre o investimento realizado, confrontando-o com os danos estimados.

Cálculo da probabilidade

É um cálculo bastante difícil sob o ponto de vista de que ele leva em consideração os registros anteriores de eventos ocorridos. Uma vez que os dados estatísticos não apresentem a real situação devido ao problema da subnotificação, esse cálculo poderá ser subestimado, induzindo a organização a um erro na determinação dessa taxa. Geralmente, para o cálculo dessa taxa, utiliza-se a média ponderada e o desvio padrão.

Cálculo das consequências

O cálculo das consequências é realizado sobre as expectativas de perdas. Ele é feito com base no valor total dos danos ou de receitas que podem ser perdidas em decorrência do evento, acrescido dos diversos gastos adicionais gerados por tal evento. Pode ser feito com base em período anual ou dentro do período de revisão do processo de análise.

O problema da utilização desse método relaciona-se com a credibilidade das fontes de informação e a disponibilidade de dados. Dessa forma, faz-se necessária uma atenção especial no momento da utilização das fontes dos dados, principalmente nos registros de eventos passados, que é uma das fontes utilizadas para estimar a probabilidade de eventos futuros, para não incorrer em valores subavaliados.

Como se pode concluir, o método não deve ser aplicado quando não há dados históricos confiáveis e quando os ativos envolvidos são de difícil mensuração. Em contrapartida, quando existe disponibilidade de informação e grande confiabilidade, a aplicabilidade desse método é bastante eficaz.

As principais vantagens e desvantagens do método quantitativo são (Microsoft, 2005):

Benefícios:

- ✓ Os riscos são priorizados de acordo com o impacto financeiro; os ativos são priorizados de acordo com os valores financeiros.
- ✓ Os resultados facilitam o gerenciamento de riscos graças ao retorno do investimento em segurança.
- ✓ Os resultados podem ser expressos usando-se uma terminologia de gerenciamento (por exemplo, valores monetários e probabilidade expressa como uma porcentagem específica).
- ✓ A precisão tende a aumentar com o passar do tempo, à medida que a organização coleta registros históricos dos dados e ganha experiência.

Desvantagens:

- ✓ O processo, para atingir resultados confiáveis e um consenso, é demorado.
- ✓ Os cálculos podem ser complexos e demorados.
- ✓ Os resultados são apresentados em termos monetários e podem ser difíceis de ser interpretados por pessoas sem conhecimento técnico.
- ✓ O processo exige experiência e conhecimento, portanto pode ser difícil explicá-lo aos participantes.

Método qualitativo

A análise qualitativa é qualquer método de análise que utiliza mais a descrição do que os recursos numéricos para definir o nível de risco (HB

436:2004). Em outras palavras, é um método de análise de riscos que utiliza valores nominais para descrever o risco.

Ele é utilizado quando não há disponibilidade e confiança no registro dos dados, quando os seus custos não estão disponíveis, quando é impossível de mensurar com outro método, e quando não existe a necessidade da precisão do método quantitativo, dentre outros fatores.

É um método mais fácil de ser utilizado, além de possibilitar um melhor entendimento sobre os riscos, para as pessoas que participam do processo, trazendo um resultado mais duradouro. O fator diferencial desse método está na habilidade, experiência e decisão de quem conduz a análise.
Nesse método, utilizam-se palavras para descrever a magnitude das consequências e a probabilidade de ela ocorrer (AS/NZS 4360:2004). A análise é realizada pela interpretação dos analistas ou equipe multidisciplinar, ao relacionar o evento com determinados níveis de referência, em vez de se atribuir valoração numérica e monetária à análise.

Abaixo são apresentados dois exemplos de escalas para a medição das consequências e das possibilidades:

Escala para medir as consequências

Descrição	**Tipos**
Severo	Muitos objetivos não podem ser desenvolvidos
Maior	Alguns objetivos importantes não podem ser desenvolvidos
Moderado	Alguns objetivos afetados
Menor	Efeitos menores que são facilmente afetados
Insignificante	Impacto desprezível sobre objetivos

Fonte: HB 436:2004

Escala para medir as possibilidades

Nível	Descrição		Indicador de frequência
A	**Frequente**	O evento ocorrerá numa base anual	Uma vez por ano ou mais Frequente
B	**Provável**	O evento tem ocorrido várias vezes ou mais na sua carreira	Uma vez a cada 03 anos
C	**Possível**	O evento poderá ocorrer uma vez na sua carreira	Uma vez a cada 10 anos
D	**Improvável**	O evento ocorre em algum lugar, de tempo em tempo	Uma vez a cada 30 anos
E	**Raro**	Ouve-se de alguma coisa que ocorre em outra parte	Uma vez a cada 100 anos
F	**Muito raro**	Nunca tem escutado do seu acontecimento	Um em 1.000 anos
G	**Inacreditável**	Teoricamente possível, mas não se espera que ocorra	Um em 10.000 anos

Fonte: HB 436:2004

A sua desvantagem em relação ao método quantitativo é que se apresentam valores relativos, em vez de valores absolutos, contudo é um método mais fácil, e possui uma ampla linha de visibilidade para a importância do processo de gerenciamento de riscos por parte das pessoas da corporação.

As principais vantagens e desvantagens do método qualitativo são (Microsoft, 2005):

Benefícios:

- ✓ Permite a visibilidade e a compreensão da classificação de riscos.
- ✓ Maior facilidade de chegar a um consenso.
- ✓ Não é necessário quantificar a frequência da ameaça.
- ✓ Não é necessário determinar os valores financeiros dos ativos.
- ✓ Maior facilidade de envolver pessoas que não sejam especialistas em segurança.

Desvantagens:

- ✓ Os valores do impacto atribuído ao risco são baseados na opinião subjetiva dos participantes.
- ✓ Riscos graves podem não ser diferenciados o suficiente.

- ✓ Dificuldade de justificar o investimento na implementação de controles, pois não há valores básicos para realizar a análise de custo/benefício.
- ✓ Os resultados dependem da qualidade da Equipe de gerenciamento de riscos formada.

O manual de gerenciamento de riscos (HB 436:2004) apresenta o **método semiquantitativo**, cujo objetivo é produzir uma escala de *ranking* de risco mais extensa do que as apresentadas no método qualitativo. Contudo, nesse método os valores atribuídos não representam os valores reais dos riscos, os quais só devem ser obtidos quando da utilização do método quantitativo. O grande problema desse método é que ele pode não produzir uma análise confiável dos riscos quando as suas probabilidades e consequências são extremas.

Parâmetros de avaliação

Outro ponto que merece destaque é a escolha dos parâmetros a serem utilizados para a avaliação do risco e a definição dos seus níveis de aceitabilidade. Os critérios de avaliação dos riscos são indispensáveis para que seja possível estabelecer o nível de risco. Já os níveis de aceitabilidade têm o propósito de prover uma orientação para as ações de tratamento ou aceitação dos riscos.

Vários parâmetros podem ser utilizados para se estabelecerem os critérios contra os quais os riscos serão avaliados, como por exemplo: financeiros: perda da produtividade, perda de vendas, perdas de mercado, aumento do custo operacional, penalidades contratuais, etc.; de imagem organizacional: dano da marca e nome da empresa, perda da confiança dos investidores, perdas do valor de mercado, mídia negativa, etc.; social e ambiental: descrédito das ações sociais, dano ambiental, dano na saúde e bem-estar social local, etc.; pessoal: instabilidade funcional e diminuição do potencial produtivo, etc.; normativo: ações judiciais, não conformidade com padrões estabelecidos, multas contratuais, etc.

Esses critérios devem levar em consideração os tipos de consequências que serão consideradas, o modo como as possibilidades serão definidas e como serão definidos os níveis de risco.

Abaixo são apresentadas duas tabelas: uma com a descrição dos parâmetros utilizados, e outra com o nível de risco para cada parâmetro.

Quadro da descrição de categorias de impacto

CATEGORIA	DESCRIÇÃO
MORTE OU FERIMENTO	Perspectiva de morte ou ferimento como resultado de um ataque
IMPACTO ECONÔMICO	O potencial impacto econômico de um ataque
IMPACTO AMBIENTAL	O potencial impacto ambiental
SEG. PÚBLICA/ IMPACTO DEFESA	O impacto do efeito de um ataque em vários alvos, incluindo o departamento de defesa
EFEITO SIMBÓLICO	Tipo efeito moral: economia americana, sistema público, militar e bem-estar social

Quadro de níveis de impacto

CATEGORIA	MORTE/ FERIMENTO	IMPACTO ECONÔMICO	IMPACTO AMBIENTAL	DEFESA NACIONAL	EFEITO SIMBÓLICO
ALTO	> 1.000	> 100 milhões de unidades monetárias	Completa destruição de múltiplos aspectos do ecossistema em uma área ampla	Criar longos períodos de vulnerabilidade na seg. pública	Mais perdas de importantes símbolos nacionais que são internacionalmente conhecidos
MÉDIO	100 a 1.000	10 a 100 milhões de unidades monetárias	Longo tempo de dano para uma parte do ecossistema	Tempos curtos de interrupção no sistema de defesa	Maior dano ou destruição de importantes símbolos locais ou nacionais
BAIXO	0 a 100	< 10 milhões de unidades monetárias	Pequeno ou impacto mínimo no ecossistema	Impactos sem gravidade	Menor ou nenhum dano para importantes símbolos

Outra forma de se medir o risco é o estabelecimento de níveis para a consequência e suas possibilidades, e a relação entre eles, pois, por definição, o risco é a combinação das possibilidades de um evento e suas consequências. De uma maneira geral, esses parâmetros servem para medir as consequências, para que, em combinação com as possibilidades, possam ser avaliados os

riscos, a fim de se estabelecer um *ranking* de prioridades com base nos níveis de aceitabilidade estabelecidos.

As tabelas abaixo exemplificam essa situação.

Exemplo de níveis de **Consequências** ou **Impactos**

Nível	Descrição	Tipos
1	**Insignificante**	Nenhum prejuízo na imagem, perdas financeiras irrelevantes, sem impactos sobre os negócios
2	**Menor**	Pequenos efeitos e facilmente reparados, ações preliminares para tratamento, solução imediata local, perdas financeiras médias
3	**Moderado**	Efeitos sobre algumas atividades de negócios, possui solução local com ajuda externa, perdas financeiras moderadas
4	**Maior**	Grandes abalos na imagem, interrupção temporária da atividade de negócio, ajuda externa para tratamento, perdas financeiras elevadas
5	**Catastrófico**	Morte, interrupção total das atividades, solução externa, danos de difícil reparação, perdas financeiras elevadas

Exemplo de níveis de **Possibilidades**

Nível	Descrição	Tipos
A	**Frequente**	É esperado que ocorra em mais circunstâncias – possibilidades de incidentes repetidos
B	**Provável**	Provavelmente ocorrerá em mais circunstâncias – possibilidade de incidentes isolados
C	**Ocasional**	Poderá ocorrer em algum tempo- possibilidade de algumas ocorrências
D	**Remota**	Ocorrerá alguma vez – ocorrência pouco provável
E	**Improvável**	Ocorrerá em circunstâncias excepcionais – praticamente impossível

A adoção de uma matriz de riscos é importante para se visualizar graficamente a relação entre as possibilidades e suas consequências, e possibilitar uma identificação mais fácil dos riscos, como está exemplificado no quadro abaixo.

Matriz de riscos (consequências X possibilidade)

	Consequências				
Possibilidade	**Insignificante 1**	**Menor 2**	**Moderado 3**	**Maior 4**	**Catastrófico 5**
A (Frequente)	A	A	E	E	E
B (Provável)	M	A	A	E	E
C (Ocasional)	B	M	A	E	E
D (Remota)	B	B	M	A	E
E (Improvável)	B	B	M	A	A

Com base nos níveis de criticidade dos riscos, eles devem ser confrontados com os níveis de aceitabilidade definidos pela organização, realizando assim a sua avaliação, como está exemplificado no quadro abaixo.

Quadro da aceitabilidade dos riscos

Risco extremo (E)	Inaceitável- requer ação corretiva imediata
Risco alto (A)	Inaceitável - requer ação corretiva imediata com atenção específica da direção
Risco moderado (M)	Inaceitável- requer monitoramento, ações de mitigação e revisão dos controles pelo gerente Aceitável – requer a revisão e autorização do gerente
Risco baixo (B)	Aceitável- requer procedimentos de rotina

Uma atenção especial deve ser dispensada à classificação dos riscos de baixa probabilidade e alto impacto. Esses riscos tendem a ser descartados. Entretanto, quando se materializam, pegam a organização despreparada, o que ocasiona enorme prejuízo.

Mesmo considerando as escalas de mensuração dos métodos de análise, entendemos ser necessário que a organização observe se esses parâmetros apresentados condizem com a sua realidade, pois muitas vezes um mesmo nível referencial de impacto não representa a mesma situação para empresas de um mesmo segmento, e até do mesmo porte.

Essa diferença é bastante clara quando se observa a classificação em valores absolutos entre empresas de porte e faturamento diferentes, e de um mesmo segmento de atividade. Nesses casos, é necessário um ajuste nos termos valorativos das tabelas de referência, para que o risco analisado não seja indevidamente avaliado como sendo de uma classificação diferente da realidade. Esse ajuste não deve ser feito para um tipo de risco específico, mas para todo um referencial de mensuração que deve ser aplicado para todos os riscos e por toda a organização, durante a avaliação.

Um cuidado especial deve haver com relação à escolha do método e dos parâmetros para o estudo do risco, para que eles não sejam escolhidos de forma negligente, por ser um método mais simples e fácil, sem a consideração que merece.

Dessa forma, faz-se necessário estabelecer condições tais que evitem uma escolha equivocada do método, e que os critérios de parametrização da criticidade dos riscos sejam ajustados à realidade da empresa. Essa escolha deve ser feita considerando, principalmente, o porte da empresa, a natureza da atividade de negócio e o seu contexto, o escopo e o objetivo do estudo do risco, dentre outros fatores.

Esses métodos e parâmetros devem ser questionados sobre o porquê de sua utilização, e quais os benefícios que podem trazer para a organização. Essa decisão quanto à escolha deve ser aprovada pelo *staff* da empresa, porque o estudo do risco é uma das etapas mais importantes do macroprocesso de gerenciamento de riscos.

3. GERENCIAMENTO DE RISCOS

Como já foi visto, o risco é medido pela probabilidade e suas consequências, e o seu estudo deve considerar, dentre outros fatores, a metodologia de análise e os critérios de parametrização. Sabe-se, também, que ele é inerente ao ambiente de negócios, que é altamente mutável.

Toda essa instabilidade contextual requer uma vigilância constante sobre esse cenário e, principalmente, sobre os seus riscos, com o objetivo de garantir uma constante harmonia entre eles (os negócios e os riscos). E essa coerência pode ser alcançada por meio do gerenciamento de riscos.

De uma maneira geral, o gerenciamento de riscos é um processo voltado para o controle dos riscos e envolve um conjunto de atividades específicas que objetivam garantir a boa governança, sem que os riscos e surpresas indesejáveis atrapalhem o alcance dos seus objetivos e metas.

O gerenciamento de riscos compreende as atividades coordenadas para dirigir e controlar a organização em relação aos riscos. O seu sistema de gerenciamento engloba o conjunto de elementos do sistema de gerenciamento da organização, que incluem o planejamento estratégico, os tomadores de decisões, e outros processos que lidam com riscos (ISO/IEC Guide 73:2002).

O gerenciamento de riscos compreende a cultura, os processos e a estrutura direcionada para potencializar as oportunidades, enquanto são gerenciados os efeitos adversos. Ele é realizado pela aplicação sistemática da gestão de políticas, procedimentos e práticas voltados para as atividades de: comunicação; estabelecimento do contexto; identificação; análise; avaliação; tratamento; monitoramento e revisão dos riscos (AS/NZS 4360:2004).

3.1 Benefícios e fatores críticos de sucesso para a gestão de riscos

Para que o processo de gerenciamento de riscos possa alcançar os seus objetivos, torna-se necessário identificar as principais variáveis que influenciam diretamente no seu desempenho, ou seja, os seus fatores críticos de sucesso.

Fatores críticos de sucesso

A Microsoft (2005) apresenta os seguintes fatores críticos para o sucesso do gerenciamento de riscos: patrocínio da alta gestão; maturidade corporativa em relação ao gerenciamento de riscos; atmosfera de comunicação aberta; espírito de equipe; visão holística e autoridade da equipe de gerenciamento de riscos.

O Órgão Geral de Auditoria e Investigação do Congresso Americano (General Accounting Office - GAO), no estudo realizado com organizações líderes de mercado, identificou alguns fatores críticos de sucesso no processo de gerenciamento de riscos, que foram: obter apoio e envolvimento dos executivos; estabelecer um ponto de apoio para todo o processo; definir os procedimentos para padronizar a avaliação de riscos; envolver os especialistas das várias unidades de negócios; estabelecer uma unidade de negócio responsável por iniciar e conduzir a avaliação de riscos; definir o escopo das avaliações e documentar e monitorar os resultados (GAO, 1999).

O manual de gerenciamento de riscos (HB 436:2004) apresenta alguns requisitos importantes para o sucesso da gestão de risco, que são: conhecimento consistente; pensamento voltado para os acontecimentos futuros e não apenas para os eventos passados; responsabilidade nas tomadas de decisão; comunicação permanente com as partes envolvidas no processo de gestão de risco e nas atividades principais da organização, e decisões baseadas no equilíbrio entre os custos e as oportunidades.

Os principais fatores que identificamos serem importantes para o sucesso do gerenciamento de riscos são:

- ✓ O patrocínio da diretoria da organização;
- ✓ A definição dos requisitos do gerenciamento alinhado com a missão e os objetivos da empresa;
- ✓ O estabelecimento do escopo de todo o processo;
- ✓ O ambiente das atividades de negócios e a criticidade do produto;
- ✓ A definição de uma equipe multidisciplinar para o macroprocesso e suas responsabilidades definidas;
- ✓ A definição dos colaboradores de diversas áreas da organização e as suas atribuições no processo;
- ✓ A forma da comunicação interna;

- ✓ A cultura da segurança da informação;
- ✓ A identificação dos principais ativos e processos de negócios;
- ✓ A confiabilidade da lista das principais ameaças à segurança da informação;
- ✓ A escolha e a utilização do método de análise dos riscos;
- ✓ Os critérios de parametrização para a classificação dos riscos e as medidas de tratamento;
- ✓ A implementação das medidas para o tratamento dos riscos;
- ✓ O controle e o monitoramento constante do processo.

A visualização desses fatores é o ponto fundamental para se alcançarem os benefícios da gestão de riscos.

Benefícios

O manual de gerenciamento de riscos (HB 436:2004) apresenta os seguintes benefícios do gerenciamento de riscos: poucas surpresas; exploração de oportunidades; planejamento, desempenho, e eficácia; economia e eficiência; relacionamento entre as partes interessadas (*stakeholder*); tomadas de decisão com informações mais exatas; manutenção da reputação; proteção dos diretores; responsabilidade, garantia e governança; e bem-estar pessoal.

Um dos principais benefícios da gestão de risco é poder garantir o desenvolvimento das atividades de negócios dentro de um ambiente de controle permanente sobre os riscos, pois, como é de conhecimento de todos, o ambiente de negócios é altamente mutável e repleto de incertezas. E a capacidade de convivência nesse cenário, mediante um processo austero de gestão, é um fator decisivo de vantagem competitiva e de sucesso nos negócios.

A atenção aos fatores críticos de sucesso e a visão do alcance dos benefícios da gestão de risco devem ser uma preocupação permanente em cada etapa do processo de gerenciamento de riscos.

3.2 Modelos de gerenciamento de riscos

Como já foi visto, o gerenciamento de riscos é um processo que comporta um conjunto de atividades voltadas para o controle dos riscos. Esse processo possui fases específicas que variam de acordo com o modelo escolhido.

Neste capítulo serão apresentados alguns modelos de gerenciamento de riscos e suas etapas.

3.2.1 Modelo segundo a norma ISO Guide 73:2002[22]

De acordo com as definições estabelecidas na norma ISO/IEC Guide 73:2002, o gerenciamento de riscos envolve as seguintes etapas: a avaliação de riscos (risk assessment), o tratamento do risco, a aceitação do risco e a comunicação do risco.

Avaliação de riscos

A avaliação de riscos (*risk assessment*) envolve a análise de riscos (*risk analysis*) e a sua avaliação (*risk evaluation*) por determinado critério para se estabelecer o nível de criticidade do risco.

Tratamento do risco

O tratamento do risco (*risk treatment*) compreende as ações para modificar o risco. É a fase da tomada de decisão quanto aos riscos que afetam a organização.

Aceitação do risco

A aceitação do risco (*risk acceptance*) está relacionada com a capacidade da empresa de aceitar determinado risco. É a decisão de aceitar o risco.

[22] Essa norma é um guia que estabelece a terminologia, as definições e as atividades relacionadas com o gerenciamento de riscos.

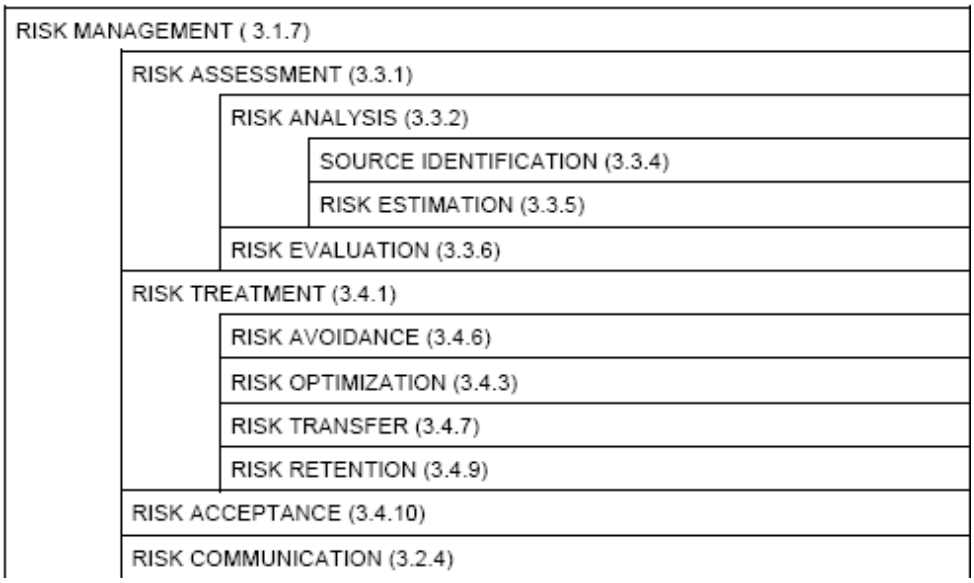
Aceita-se um risco quando as suas probabilidades e consequências são muito baixas ou desprezíveis, e as contramedidas não forem financeiramente viáveis.

Comunicação do risco

A comunicação do risco envolve a troca ou compartilhamento da informação dos seus riscos com tomadores de decisões, *stakeholders* e grupos de respostas a incidentes de proteção.

A comunicação é importante para o aperfeiçoamento das equipes e instituições envolvidas, e tem como resultado o aumento da capacidade de resposta, seja na redução do tempo de resposta a um evento, seja na medida a ser adotada. Ela proporciona o desenvolvimento de uma *network* cada vez mais estruturada para enfrentar os riscos.

Abaixo reproduzimos a figura que permite visualizar a relação entre as diversas etapas do gerenciamento de riscos.



Fonte: ISO/IEC Guide 73:2002.

3.2.2 Modelo segundo a norma AS/NZS 4360:2004[23]

A norma AS/NZS 4360:2004 estabelece as seguintes etapas para o processo de gerenciamento de riscos: comunicação e consulta; estabelecer o contexto; avaliar o risco (*risk assessment*); tratar o risco, e monitorar e revisar.

Comunicação e consulta

Esta etapa possui uma característica peculiar por interagir com as outras fases durante todo o processo. Caracteriza-se por estabelecer uma troca de informações constante e interativa entre as partes envolvidas durante todo o processo de gestão dos riscos.

Essa interação, além de obter uma variedade de opiniões de seus agentes intervenientes, proporciona a compreensão por parte das pessoas quanto ao que representa o risco, bem como a importância do seu processo de gestão para a organização.

Estabelecer o contexto

Esta etapa envolve as atividades de estabelecimento dos contextos interno externo e do contexto do gerenciamento de riscos, o desenvolvimento dos critérios de avaliação dos riscos e a estrutura desse processo de gestão.

O contexto do gerenciamento de riscos deve estar alinhado com o ambiente de negócios da organização, o qual deve ter sido estabelecido no planejamento estratégico. Entretanto, quando do início dessa fase, pode ser que o contexto definido anteriormente no planejamento estratégico necessite de ajustes. Nessa fase, o escopo, os objetivos, as metas e atividades de todo o processo são estabelecidos, inclusive os recursos necessários à sua realização.

Os critérios para a avaliação dos riscos (*risk evaluation*) são desenvolvidos nessa fase, como também é identificada toda a estrutura de trabalho necessária à consecução das atividades do processo de gestão dos riscos.

[23] Esta norma fornece um guia genérico para o gerenciamento de riscos. É o padrão seguido pela Austrália (AS) e Nova Zelândia (NZS).

Avaliação de riscos

Nesta etapa, os riscos são identificados, analisados e avaliados de acordo com critérios previamente estabelecidos. É realizada em 3 fases: identificar os riscos, analisar os riscos, e avaliar os riscos (*risk evaluate*).

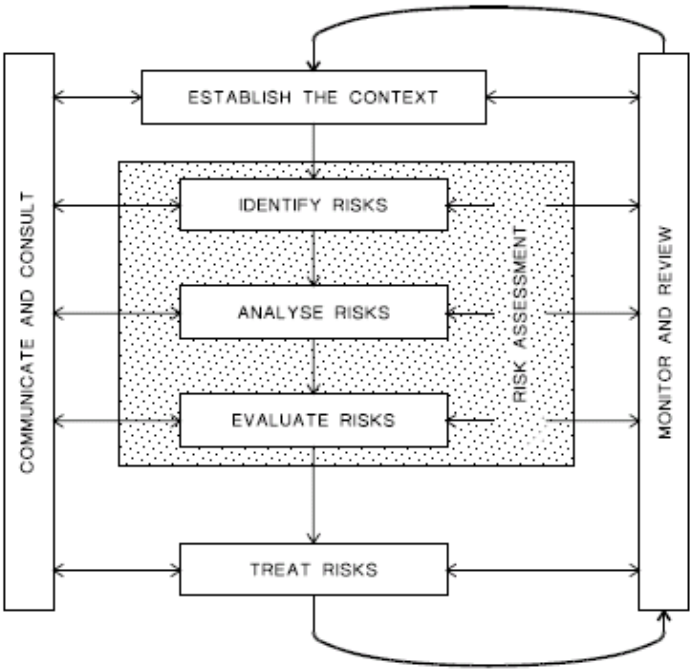
Tratar o risco

Esta fase compreende ações específicas para reduzir perdas potenciais e aumentar os seus benefícios ao se tomar a melhor decisão quanto aos riscos avaliados.

Monitorar e rever

Esta fase também possui a característica específica de interagir em todas as fases do processo de gestão de risco, pois a efetividade do gerenciamento requer um monitoramento permanente, bem como uma revisão das medidas de tratamento para aferir a sua eficiência e eficácia.

A figura abaixo representa todo esse processo:



Fonte: AS/NZS 4360:2004

3.2.3 Modelo de gerenciamento de riscos de segurança da Microsoft

Para a Microsoft, o gerenciamento de riscos de segurança é o processo de determinação de um nível de risco aceitável que envolve avaliar o nível de risco atual, tomar medidas para reduzir o risco a um nível aceitável e manter esse nível de risco (Microsoft, 2005).

O processo de gerenciamento de riscos de segurança da Microsoft é dividido em quatro fases: avaliando os riscos; oferecendo suporte às decisões; implementando controles e analisando a eficácia do programa.

A primeira fase do seu processo de gerenciamento de riscos é a etapa de **avaliando os riscos**. Nessa fase são combinados aspectos dos métodos quantitativo e qualitativo de análise de riscos. Uma abordagem qualitativa é usada para filtrar rapidamente a lista completa dos riscos de segurança.

Os riscos mais graves são identificados durante essa filtragem e, em seguida, são examinados em detalhe, usando-se uma abordagem quantitativa. O resultado é uma lista relativamente curta que contém os riscos mais importantes que já foram examinados em detalhe.

A lista dos riscos mais importantes é usada durante a segunda fase, **oferecendo suporte às decisões**, na qual um conjunto de possíveis soluções de controle é proposto e examinado, apresentando as melhores propostas ao comitê de orientação de segurança da organização como recomendações para a atenuação desses riscos.

Durante a terceira fase, **implementando controles**, os proprietários são responsáveis por implementar as soluções de controle escolhidas.

Na quarta fase, **analisando a eficácia do programa**, é verificado se os controles oferecem de fato o grau de proteção esperado, além de se monitorarem as alterações no ambiente, como, por exemplo, a instalação de novos aplicativos de negócios ou ferramentas de ataque que possam alterar o perfil de risco da organização.

Como o processo de gerenciamento de riscos de segurança da Microsoft é um processo contínuo, o ciclo é reiniciado com cada nova avaliação de riscos. A frequência com que o ciclo é reiniciado varia de acordo com a organização: diversas empresas acreditam que uma recorrência anual é suficiente, desde que a organização esteja monitorando de forma proativa as novas vulnerabilidades, ameaças e ativos.

Abaixo está reproduzida a figura que ilustra as quatro fases do processo de gerenciamento de riscos de segurança da Microsoft.

Fonte: Guia de Gerenciamento de riscos de Segurança.

3.2.4 Modelo segundo a norma BS 7799-3:2006

A norma BS 7799-3:2006 fornece orientação e recomendações para as atividades de gerenciamento de riscos do sistema de gestão de segurança da informação (Information Security Management System- ISMS), em conformidade com os requisitos estabelecidos na norma BS 27001:2005,[24] que dentre outras coisas estabelece os requisitos para as atividades associadas ao gerenciamento de riscos.

O padrão britânico (*British Standard*) de gerenciamento de riscos adota a abordagem por processos, que encoraja os seus usuários a enfatizarem a importância de: a- Entendimento dos requisitos de segurança da informação dos negócios e a necessidade de se estabelecerem políticas e objetivos para a segurança da informação; b- Selecionar, implementar e

[24] A norma BS 27001:2005, assim como a ISO 27001:2005, prover um modelo para estabelecer, implementar, operar, monitorar e revisar, manter e melhorar um ISMS.

operar controles selecionados no contexto do gerenciamento de todos os riscos de negócios da organização; c- Monitorar e revisar o desempenho e eficácia do ISMS para gerenciar os riscos dos negócios; d- Desenvolver a melhoria contínua, baseada na medição objetiva dos riscos.

O seu processo de gerenciamento de riscos compreende as seguintes etapas:

1. Avaliar os riscos;
2. Tratar os riscos;
3. Monitorar e revisar os riscos;
4. Manter e melhorar o sistema de controle dos riscos.

Avaliar os riscos

Esta fase compreende o processo de avaliação de riscos e inclui a análise e a avaliação (*evaluation*) dos riscos. Para se analisarem os riscos são desenvolvidas as seguintes atividades: a identificação dos riscos; a identificação dos requisitos legais e de negócios que são relevantes para os ativos identificados; a valoração dos ativos identificados, considerando a classificação dos seus requisitos e as expectativas de perda de confidencialidade, integridade e disponibilidade; a identificação das principais ameaças e vulnerabilidades; a avaliação da possibilidade de ameaças e vulnerabilidades ocorrerem.

Para avaliar (*evaluation*) os riscos são realizados o cálculo do risco para poder avaliá-los contra o critério predefinido.

Tratar os riscos

Nesta fase são tomadas as decisões para melhor gerenciar os riscos, por meio de controles de prevenção e detecção, além de medidas para se evitarem e transferirem riscos. Essas decisões devem ser registradas e materializadas no plano de tratamento dos riscos. É o processo clássico de tratamento dos riscos, como foi visto nos modelos apresentados anteriormente.

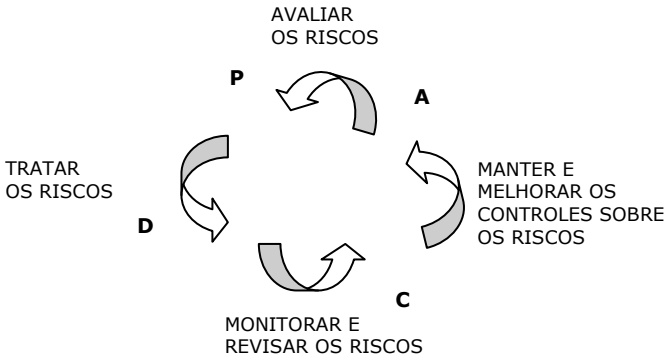
Monitorar e revisar

É nesta etapa onde ocorrem as atividades que garantem o funcionamento eficaz dos controles implementados. Como os controles

podem ser deteriorados ou ficar obsoletos com o passar do tempo, são indispensáveis ações para garantir o seu pleno funcionamento e a sua eficácia.

Manter e melhorar

Esta fase alcança as atividades que previnem e corrigem as falhas e deficiências encontradas durante o monitoramento e a revisão (análise crítica). É nela que são executas as ações preventivas e corretivas.
A figura abaixo representa esse modelo de gerenciamento de riscos:



Fonte: BS 7799-3:2006

Como se pode observar, essa norma estabelece o modelo PDCA para o gerenciamento de riscos, identificado na figura acima, pelas iniciais de cada etapa: *Plan* (P), Do (D), *Check* (C) e *Act* (A), ou seja, na fase de planejamento (P) ocorre a definição do escopo do gerenciamento, a escolha do método de análise e o processo geral de avaliação de riscos; na fase de execução (D), temos o tratamento de risco, com a implementação dos controles relacionados para prevenir, detectar, evitar, aceitar e transferir os riscos; na fase de verificação (C), ocorrem as atividades de monitoramento e revisão desse processo; na fase da ação (A) ocorrem as ações para que o sistema possa ser mantido e melhorado continuamente, dando origem às ações preventivas e corretivas.

3.2.5 Modelo segundo o IT Governance Institute (COBIT® 4.1)

O IT Governance Institute,[25] com a publicação do Control Objectives for Information and related Technology (COBIT® 4.1), fornece boas práticas por meio de uma estrutura de processos, domínios e atividades de controle voltadas para a boa governança nos serviços de TI. Em um de seus domínios[26] encontra-se o seu modelo de avaliação e gestão de riscos.

Esse modelo apresenta as seguintes etapas: estabelecer a estrutura de gerenciamento de riscos de TI; estabelecer o contexto dos riscos; identificar os eventos; avaliar os riscos; responder aos riscos, e manter e monitorar o plano de ação dos riscos.

Estabelecer a estrutura de gerenciamento de riscos

Esta fase requer que a estrutura para gerenciar os riscos de TI esteja alinhada com a estrutura de gestão de riscos totais da organização.

Estabelecer o contexto dos riscos

É a fase na qual são desenvolvidas atividades para que o resultado da avaliação de riscos produza resultados apropriados. É nesta fase que são identificados o cenário (ambiente interno e externo), as metas da avaliação e são definidos os critérios segundo os quais os riscos serão avaliados.

Identificar os eventos

Como o próprio nome já diz, é nesta fase que os eventos são identificados com as suas probabilidades e consequências, ou seja, é a fase da

[25] IT Governance Institute foi criado em 1998 para o desenvolvimento e padronização de uma estrutura de controle direcionada para os serviços de tecnologia da informação. E esse padrão é estabelecido por meio do COBIT, que é uma publicação robusta, que serve como guia para se estabelecer uma estrutura (*framework*) com as melhores práticas para a governança, controle e auditoria dos serviços de TI. O COBIT fornece suporte ao Commitee of Sponsoring Organizations of the Treadway Commission (COSO), em que a uma entidade criada para estudar os casos de fraudes em relatórios financeiros, cujo foco dos seus trabalhos são os controles internos e os relatórios financeiros.

[26] Os quatro domínios do COBIT são: planejar e organizar; adquirir e implementar; entregar e suporte, e monitorar e avaliar. O processo de avaliação e gestão de riscos faz parte do domínio planejar e organizar.

identificação dos riscos, uma vez que os riscos são medidos pelas suas probabilidades e consequências.

Avaliar os riscos

É nesta fase que ocorre a avaliação dos riscos identificados.

Responder aos riscos

É a fase na qual são desenvolvidos os processos para responder aos riscos avaliados. É a fase na qual ocorre o tratamento dos riscos com estratégias para evitar, reduzir, compartilhar ou aceitar os riscos.

Manter e monitorar o plano de ação dos riscos

É quando ocorre o monitoramento de todas as atividades de controle, de modo a se fazerem as alterações necessárias ao gerenciamento dos riscos de TI.

3.2.6 Modelo segundo a norma ISO 27005:2008

A norma ISO 27005:2008 fornece diretrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo particularmente aos requisitos de um sistema de gestão de segurança da informação de acordo com o padrão da norma ISO 27001:2005.

Esse modelo apresenta as seguintes etapas: 1- Definição do contexto; 2- Avaliação de riscos (*risk assessment*), com as etapas de análise de riscos e avaliação de riscos (*risk evaluate*); 3- Tratamento de risco; 4- Aceitação do risco; 5- Comunicação do risco, e 6- monitoramento e análise crítica de riscos.

O processo de gestão de riscos apresentado por essa norma é semelhante ao da AS/NZS 4360:2004, e sua representação gráfica é a mesma. Seu processo de gestão de riscos é alinhado com o processo do sistema de gestão de segurança da informação de acordo com o padrão estabelecido na norma ISO 27001:2005, que adota o sistema PDCA. A tabela abaixo identifica essa relação:

Processo do SGSI	Processo de Gestão de Riscos de Segurança da Informação
Planejar **(P)**	Definição do contexto; avaliação de riscos (*risk assessment*); definição do plano de tratamento do risco; aceitação do risco.
Executar **(D)**	Implementação do plano de tratamento do risco.
Verificar **(C)**	Monitoramento contínuo e análise crítica de riscos.
Agir **(A)**	Manter e melhorar o processo de gestão de riscos de segurança da informação.

Fonte: Norma ABNT ISO/IEC 27005:2008

Observe-se que essa norma foi elaborada para atender a uma demanda específica daquelas organizações que pretendem certificar seus sistemas de gestão de segurança da informação com o padrão da norma ISO 27001:2005. Entretanto, para se atender ao requisito dessa norma (27001:2005), não se faz necessário adotar o modelo aqui apresentado, pois a norma BS 7799-3:2006 também satisfaz a esse requisito, uma vez que ambas as normas fornecem um suporte para que as organizações possam montar o seu sistema de gestão de segurança da informação alinhado com os requisitos indispensáveis da norma ISO 27001:2005.

3.3 O processo de avaliação de riscos

Como pôde ser visto, a avaliação de riscos é um processo geral de análise e avaliação, que no final apresenta uma relação com os seus principais riscos, apontando a necessidade de tratamento específico para cada um deles.

Este capítulo é dedicado a esse processo que, como vimos, é parte integrante do macroprocesso de gestão de riscos.

Objetivos da avaliação de riscos

O objetivo do processo de avaliação de riscos é identificar, analisar e avaliar os riscos.

Com a finalidade de alcançar seus objetivos, esse processo deve estar alinhado com o ambiente e requisitos de negócios, para que os riscos possam ser avaliados dentro de critérios que representem a real demanda da organização.

As avaliações de risco devem ser realizadas para a identificação, quantificação e priorização dos riscos, com base em critérios estabelecidos para a aceitação, e também nos objetivos relevantes para a organização (NBR ISO/IEC 27002:2005).

Para que isso seja possível, devem ser identificados os principais processos de negócios e seus ativos, suas vulnerabilidade e ameaças, para serem utilizados na análise da probabilidade e consequência do risco, para o estabelecimento de um nível de criticidade, para serem comparados com os critérios estabelecidos, proporcionando transparência às ações para tratamento. Todas essas atividades são desenvolvidas em etapas específicas.

Etapas da avaliação de riscos

As etapas da avaliação de riscos variam de acordo com o modelo escolhido.

O Guia de gerenciamento de riscos de segurança da Microsoft (Microsoft, 2005) apresenta as seguintes etapas para a avaliação de riscos: determinar ativos e identificar cenários organizacionais; identificar ameaças; identificar vulnerabilidades; estimar a exposição dos ativos; estimar a probabilidade das ameaças, e identificar os controles existentes e a probabilidade de exploração.

A Guarda Costeira Americana (United States Coast Guard, 2003) estabelece as seguintes etapas para uma avaliação de riscos: avaliação crítica; avaliação da ameaça; avaliação da consequência e da ameaça; categorizar a avaliação alvo/cenário, e definir estratégias para mitigar e implementar medidas.

As normas ISO/IEC Guide 73 e BSI 7799-3:2005 estabelecem duas etapas para a avaliação de riscos: a análise do risco e a avaliação do risco (risk evaluation). Já a norma AS/NZS 4360:2004 apresenta 3 etapas para a avaliação de riscos: identificar os riscos, analisar os riscos e avaliar os riscos (*risk evaluate*). A diferença entre as fases dessas normas está no fato de a identificação do risco ocorrer dentro da fase da análise (ISO Guide), quando a

norma (AS/NZS) dispensa tratamento específico como etapa própria (identificar os riscos). Contudo, no contexto geral do processo de avaliação, elas possuem a mesma finalidade.

A escolha de um método de avaliação é um dos requisitos exigidos pela norma ISO 27001:2005, para se estabelecer um sistema de gestão da segurança da informação. Essa metodologia deve ser adequada aos requisitos legais, regulamentares e de segurança da informação identificados para o negócio.

Independentemente da escolha do modelo, 3 fases destacam-se durante a avaliação de riscos: identificar os riscos, analisar os riscos e avaliar os riscos.

3.3.1 Identificar os riscos

Na fase de identificação dos riscos, as atividades são direcionadas para identificar onde, quando, o porquê e como os eventos podem ocorrer de forma a prejudicar as atividades de negócio da organização. O seu resultado é materializado em uma relação com os riscos e suas fontes.

A norma ISO 27001:2005 estabelece que, ao identificar os riscos, a organização deve: 1) Identificar os ativos dentro do escopo do ISMS e os proprietários desses ativos; 2) Identificar as ameaças a esses ativos; 3) Identificar as vulnerabilidades que podem ser exploradas pelas ameaças, e 4) Identificar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.

Identificar os ativos e seus proprietários

Esta é a fase em que são identificados os ativos e seus proprietários, o que resulta em um inventário de todos os ativos do ISMS, seus proprietários e um valor atribuído para cada ativo que expresse a sua importância em relação à perda do requisito de segurança estabelecido.

Como já foi visto no primeiro capítulo, a norma ISO 27002:2005 apresenta alguns tipos de ativos relacionados com os sistemas de informação, que são:

> **Ativos de informação**: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre

pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilas de auditoria e informações armazenadas;
Ativos de *software*: aplicativos, sistemas de uma forma geral, ferramentas de desenvolvimento e utilitários;
Ativos físicos: equipamentos computacionais (processadores, monitores, *laptops*, *modens*), equipamentos de comunicação (roteadores, PABXs, fax, secretárias eletrônicas), mídia magnética (fitas e discos), mídias removíveis e outros equipamentos técnicos (*no-breaks*, ar-condicionado), mobília, acomodações;
Serviços: computação e serviços de comunicação, utilidades gerais, por exemplo, aquecimento, iluminação, eletricidade, refrigeração;
Pessoas: pessoas e suas qualificações, habilidades e experiências;
Intangíveis: reputação e imagem da organização.

A identificação dos ativos por si só não é suficiente, pois se torna necessário atribuir-lhe um valor de importância que ele representa para a organização em relação aos possíveis danos de um evento indesejável.

Existem várias técnicas para se atribuir um valor ao ativo. Uma técnica que pode ser utilizada para facilitar essa valoração é conhecer quais são os fatores críticos para o sucesso[27] da empresa.

Por exemplo, uma empresa que fornece serviços pela internet tem como fatores críticos para o seu sucesso a sua imagem e reputação no mercado, a qualidade dos serviços (especialmente a logística e a especificação do produto de acordo como o pedido feito), o sigilo dos dados de seus clientes, a disponibilidade dos seus serviços a qualquer momento em que o cliente acesse os serviços e a praticidade de acesso.

Após identificar os principais processos de negócios, deve ser feita uma classificação para se estabelecer a criticidade dessas atividades. Essa classificação pode ser feita com base nos níveis estratégico, tático e

[27] Os fatores críticos de sucesso nesta etapa não são os fatores críticos de sucesso da análise de risco, e sim para os negócios corporativos.

operacional, ou com base no custo de interrupção, ou em outros fatores definidos pela empresa.

Abaixo apresentamos a classificação utilizada por Toigo (2003) para as atividades de negócios:

> **Crítica**: funções que não podem ser desenvolvidas, a não ser que capacidades identificadas formem uma base para repor a capacidade de perigo da companhia. Aplicações críticas não podem ser repostas por métodos manuais sob nenhuma circunstância. A tolerância para a interrupção é muito pouca e o custo é muito elevado.
> **Vital**: funções que não podem ser desenvolvidas por meios manuais, ou podem ser desenvolvidas manualmente por apenas um breve período de tempo.
> **Sensível**: funções que podem ser realizadas com dificuldade e custo tolerável, por meios manuais e por um extenso período de tempo.
> **Não crítico**: funções que podem ser interrompidas por um longo período de tempo, com pouco ou nenhum custo para a companhia.

Nessa técnica, após classificar a criticidade da atividade de negócio, devem ser identificados os ativos que compõem cada uma de suas atividades, para se poder estabelecer um valor para cada um deles.

Essa valoração pode ser expressa: em termos da sua importância, como na classificação apresentada acima; em termos dos requisitos de segurança (confidencialidade, integridade e disponibilidade) em relação aos impactos provocados pela quebra desses requisitos, como: divulgação, indisponibilidade, modificação e destruição da informação; em termos financeiros, com base no custo de manutenção, reparação e/ou reposição; em termos do custo do tempo de interrupção, etc.

A valoração financeira do ativo pode ser feita com base, exclusivamente, no valor monetário de mercado para a sua reposição, ou no retorno do investimento que o valor utilizado para repor aquele ativo proporcionaria à organização (aplicações no mercado), ou no custo da captação de recursos para a nova aquisição (financiamento do ativo). Esse

fator pode ser combinado com o custo estimado da interrupção dos serviços e do prejuízo à imagem da organização pela indisponibilidade desse serviço.

Como a valoração monetária de todos os ativos para o processo de avaliação é difícil, têm-se adotado escalas de valoração nominal, que variam de 3 a 5 níveis, como, por exemplo: insignificante, baixo, médio, alto e muito alto.

O Guia de gerenciamento de riscos de segurança da Microsoft (Microsoft, 2005) apresenta 3 níveis para a classificação de ativos: impacto comercial alto, impacto comercial moderado e impacto comercial baixo. Os ativos classificados como impacto comercial alto são aqueles cujas perdas são graves ou catastróficas. Nos ativos de impacto comercial moderado são classificados aqueles cujas perdas são moderadas, e classifica como impacto comercial baixo todos aqueles não classificados nas categorias anteriores.

A norma ISO 27002:2005 orienta que devem ser levados em consideração na classificação de um ativo o seu valor, os requisitos legais, a sensibilidade e a criticidade para a organização.

Se for considerada a valoração dos ativos em relação aos impactos da quebra dos requisitos de confidencialidade, e considerando a classificação em 4 níveis, essa escala de classificação poderia ser expressa da seguinte forma:

Escala de valoração do ativo: requisito de confidencialidade

NÍVEL	DESCRIÇÃO
Baixo	Informação acessada por qualquer pessoa dentro e fora da organização. Informação classificada como pública.
Médio	Informação acessada pelo pessoal interno da organização. Informação classificada como reservada.
Alto	Informação acessada pelo nível gerencial da organização. Informação classificada como confidencial.
Muito alto	Informação acessada apenas pelos integrantes do nível estratégico da organização. Informação classificada como secreta e ultrassecreta.

Abaixo estão apresentados alguns exemplos da finalização dessa etapa, utilizando os requisitos de segurança da confidencialidade, da integridade e da disponibilidade.

Ativo: *Software* aplicativo da empresa
Identificação: Sw3
Descrição: *software* padrão utilizado por todos da organização.
Proprietário do ativo: gerente de suporte.
Requisito do ativo: *software* deve ser original e em conformidade com a legislação de direito autoral em vigor.
Descrição do requisito: o *software* adquirido é para ser utilizado apenas no trabalho, e não pode ser copiado por funcionários.
Confidencialidade: valor baixo – é o *software*-padrão da organização, não é confidencial para todos os funcionários.
Integridade: valor médio – o *software* deve funcionar corretamente, e especificamente quando processar dados dos clientes.
Disponibilidade: valor alto – o *software* deve estar disponível para todos os funcionários, em tempo integral.

Ativo: Site da empresa
Identificação: *Web site*
Descrição: *site* oficial da empresa, com a possibilidade de realização de negócios.
Proprietário do ativo: gerente de negócios.
Requisito do ativo: disponibilidade do *site*.
Descrição do requisito: o *site* e a informação contida devem estar disponíveis para os clientes poderem fazer pesquisas, solicitações e negócios que atendam às suas demandas.
Confidencialidade: valor baixo – o *Web site* deve ser acessível a qualquer cliente potencial a qualquer tempo.
Integridade: valor alto – a informação presente no *Web site* deve ser correta.
Disponibilidade: valor muito alto – o *Web site* necessita estar disponível para a demanda do cliente.

Ativo: Contratos com terceiros
Identificação: *Ct_ext*
Descrição: todos os contratos que incluam serviços prestados por terceiros e *outsourcing*.
Proprietário do ativo: gerente do setor de contratos com terceiros.

Requisito do ativo: fornecimento apropriado de serviços externos e *outsourcing*.
Descrição do requisito: o contrato deve especificar o serviço a ser prestado pela outra parte, devendo citar quais as ações e reparações se o serviço e/ou a qualidade não estiverem de acordo com o especificado no contrato.
Confidencialidade: valor alto – todos os contratos com outras partes são gerenciados pelo proprietário do ativo, e qualquer membro da organização só pode ter acesso a esses contratos com a autorização expressa do seu proprietário.
Integridade: valor muito alto – a integridade dos contratos é importante para garantir o desenvolvimento dos serviços pela outra parte, conforme foi contratado.
Disponibilidade: valor alto – os contratos devem estar disponíveis dentro de poucas horas, se eles forem necessários para verificação, renegociação, etc.

Identificar as ameaças aos ativos

Como já foi visto, a norma ISO/IEC 13335-1:2004 define ameaças como a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização. De maneira geral, as ameaças são tidas como agentes ou condições que exploram as vulnerabilidades e provocam danos.

Também foi apresentado que as ameaças podem ser naturais, acidentais e intencionais, e que, das diversas fontes sobre os tipos de ameaças, as pesquisas de segurança da informação se apresentam como fontes bastante confiáveis, lembrando que os registros de incidentes passados também são fontes bem importantes nessa fase.

Algumas técnicas podem ser utilizadas para identificar as ameaças, como, por exemplo, a utilização de ferramentas para explorar falhas de segurança, *brainstorming* e *checklists*. O objetivo é identificar o maior número de ameaças possíveis.

Contudo, o grande problema dessa etapa está diretamente relacionado com a qualidade e a confiabilidade das informações, pois cada ameaça possui certa relação com a possibilidade de sua ocorrência, que é baseada nos registros de eventos passados, além da motivação para a sua concretização e dos fatores geográficos, de maneira geral.

As manifestações mais comuns de ameaças são: erros e omissões, fraude e roubo, sabotagem de funcionário, perdas de suporte físico e de infraestrutura, atividade *hacking*, código malicioso e espionagem industrial (HB 231:2004).

A norma BS 7799-3:2006, em seu anexo "C", apresenta uma vasta lista de ameaças, dentre as quais: atos de terrorismo, falha de ar-condicionado, ataque de bomba, brechas na legislação e em contratos, compromissos de ativo e de seguranças, dano causado por testes de invasão e por outras partes, destruição de registros e de planos de continuidade, deterioração de mídia, desastres naturais ou provocados pelo homem, divulgação de informação e de senhas, erros, falha de suporte, fraudes, ação industrial, perdas, acesso não autorizado, etc.

Essas ameaças também podem ser identificadas em relação aos objetivos de controle, que são os motivos pelos quais os controles são estabelecidos. Como exemplo, abaixo, reproduzimos da norma BS 7799-3:2006 as ameaças aos objetivos do item A.9.1 (áreas seguras) do anexo A da norma ISO 27001:2005.

> Objetivo: prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações.
> Ameaças: fogo, ataque de bomba, terremoto, contaminação ambiental, inundação, furacão, ação industrial, interferência, roubo, acesso físico não autorizado e dano intencional.

Uma técnica que pode ser utilizada para facilitar a identificação das ameaças é considerar a atividade de negócio e fazer as seguintes indagações: "o quê?", "quando?", "onde?" e "qual o agente motivador?". Por exemplo, ao se considerar a atividade de projetos de novos produtos, deve-se indagar: O que poderá acontecer? Vazamento ou roubo da informação, alteração do conteúdo e dano à imagem. Quando? No momento do transporte do projeto ou de mídias com dados do projeto, ou no arquivamento desses dados. Onde? No departamento de expedição e no arquivo de mídias e documentos. Qual o agente motivador? Funcionário insatisfeito.

Outro ponto que merece atenção é a identificação das ameaças, relacionado-as por tipo de categoria: as naturais, as intencionais e as involuntárias.

Na categoria de ameaças naturais, devem ser identificadas todas aquelas decorrentes de eventos da natureza, como: fogo, inundação, tempestade, relâmpago, *tsunamis*, etc.

Na categoria de involuntárias devem ser incluídas todas as possíveis ações acidentais, como falha de equipamento, falta de energia, erro funcional, divulgação de documento, etc.

Na categoria de intencionais devem ser incluídas todas as ações deliberadas para provocar um dano à organização. Podem ser divididas em ações que causam dano às pessoas, como: incêndio criminoso, bomba, sabotagem, vandalismo; e aquelas que não causam danos às pessoas: furto, greve, espionagem, divulgação de informação. Essas subcategorias podem ser classificadas como ações intencionais violentas e não violentas, respectivamente.

Essas ameaças ainda podem ser mais discriminadas, como, por exemplo, o acesso não autorizado, que pode ser: ao estabelecimento, ao equipamento, aos relatórios, aos sistemas de informação, etc.

Como as ameaças por si só não representam o risco, pois outros fatores concorrem para tal, como os motivos da ocorrência das ameaças e a eficácia dos controles existentes, a sua avaliação passa pela identificação das vulnerabilidades, que é a próxima fase da etapa de identificação dos riscos.

Identificar as vulnerabilidades

Como já foi visto, as vulnerabilidades são fragilidades que podem provocar danos ao serem exploradas pelas ameaças. Como se sabe, tanto uma vulnerabilidade quanto uma ameaça por si só não provocam danos, pois a concretização do risco envolve um conjunto de fatores que deságuam na sua materialização.

Esses fatores geralmente estão relacionados com os processos, políticas, controles, equipamentos, *softwares*, comunicações, *hardware*, comunicações e recursos humanos, dentre outros. E a sua identificação caracteriza essa etapa.

É a etapa da identificação do risco, quando são feitas as perguntas "qual a sua causa ou motivo?", "por quê?" e "como?", para se identificar o porquê de tal acontecimento, ou seja, o fato que motivou a concretização da ameaça, e se compreender a forma pela qual ela ocorreu.

Na etapa da identificação das vulnerabilidades, devem ser identificadas as fragilidades relacionadas com os ativos no ambiente físico, nos controles e procedimentos, nas operações de negócios e fornecimento de serviços, nos *hardware*, *software* e equipamento de comunicações e instalações. (BS 7799-3:2006). Essas fragilidades podem ser identificadas por si só, ou em relação com as ameaças.

O manual HB 231:2004 apresenta uma série de exemplos de vulnerabilidades, dentre elas: **Área física e do ambiente**: falta de proteção física à instalação, portas, janelas; instabilidade da energia; localização em área susceptível à inundação; **Hardware**: susceptibilidade a variação de voltagem, de temperatura, a poeira, umidade, radiação eletromagnética; falta de controle de mudança de configuração; **Software**: falta de mecanismo de identificação e autenticação; ausência das trilhas de auditoria; tabelas de senhas desprotegidas; alocação errada de direitos de acesso; falta de documentação; falta de *backup*; **Comunicações**: linhas de comunicações desprotegidas; falta de identificação e autenticação de emissor e receptor; gestão inadequada da *network*; conexões de rede pública desprotegidas; **Documentação**: arquivo desprotegido; falta de controle para cópias; falta de cuidado na disponibilização da documentação; **Pessoal**: falta de pessoal; treinamento de segurança insuficiente; ausência de conhecimento de segurança; utilização incorreta de *software* e *hardware*; falta de mecanismo de monitoramento; ausência de políticas para a utilização correta de mídia e de mensagens; procedimento inadequado para seleção.

A norma BS 7799-3:2006 apresenta uma série de exemplos de vulnerabilidades e sua relação com possíveis ameaças, dos quais citamos apenas alguns na tabela abaixo:

Vulnerabilidade	Ameaça
Área: segurança física e do ambiente	
Descuido ou utilização inadequada do controle de acesso às instalações, salas e	Dano intencional

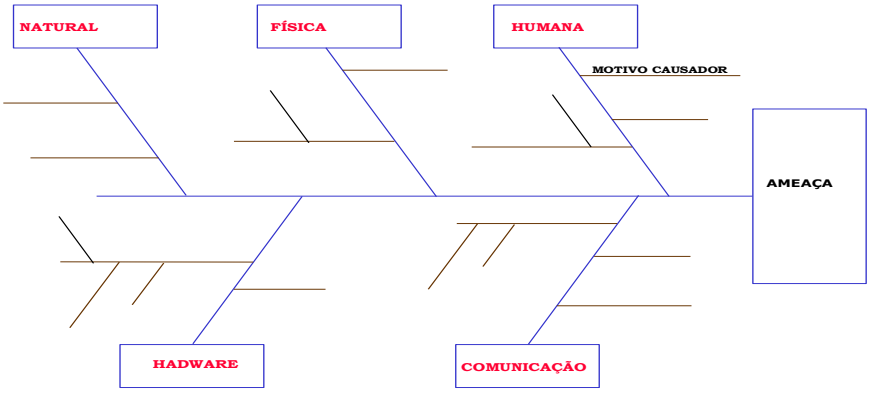
escritórios	
Arquivo desprotegido	Roubo
Área: gerenciamento das operações e comunicações	
Interface de usuário complexa	Erro operacional
Mudança inadequada de controle	Falha de segurança
Área: controle de acesso	
Segregação imprópria da *network*	Conexões não autorizadas na *network*
Falta de proteção de equipamento de computação móvel	Acesso não autorizado a informação
Área: aquisição, desenvolvimento e manutenção de sistemas de informação	
Proteção inadequada das chaves de criptografia	Revelação da informação
Seleção errada de dados para teste	Acesso não autorizado à dado/informação pessoal

Fonte: BS 7799-3:2006

Algumas ferramentas e técnicas podem ser utilizadas para identificar vulnerabilidades. As **ferramentas automatizadas** de identificação de vulnerabilidades geralmente executam uma varredura e monitoram a *network*. A utilização dessas ferramentas garante o exame periódico dos ativos e identifica fontes oportunas de vulnerabilidade.

Uma técnica utilizada para a identificação de vulnerabilidades é o emprego do diagrama de causa e efeito. Esse diagrama também é conhecido peã denominação de **diagrama de Ishikawa**, porque foi desenvolvido primeiro por Kaoro Ishikawa, em 1943, na Universidade de Tóquio; ou por diagrama Espinha de Peixe, pela sua similaridade com a forma de um esqueleto de peixe.

Esse diagrama é construído em duas etapas: a primeira descreve o problema específico, que pode ser a ameaça potencial; e a segunda pesquisa as possíveis causas, que são as vulnerabilidades. A sua construção é parecida com uma espinha de peixe, em cuja extremidade direita é colocado o problema (que no nosso caso é a ameaça), e à esquerda as categorias das principais vulnerabilidades. No final o diagrama apresenta a seguinte forma:



Nas janelas da esquerda devem ser colocadas as vulnerabilidades, por origem: natural, física, de *hardware*, de *software*, nos meios de armazenamento, humanas e nas comunicações. Com isso são analisados os possíveis motivos que concorreram para a concretização da ameaça.

Outra ferramenta importante é a auditoria, que pode ser utilizada para avaliar se os controles são eficazes, e assim mensurar se estão ou não vulneráveis. Na auditoria, o auditor deverá focar o seu exame na avaliação da eficácia dos controles em prevenir e detectar possíveis ameaças. O seu trabalho deverá estar baseado nas políticas e nos controles implementados. Ele poderá realizar o seu trabalho mediante uma análise GAP com base nos controles aplicáveis ou com base em níveis de maturidade previamente estabelecidos.

É indispensável no exame de auditoria para se identificarem vulnerabilidades que todos os registros de eventos passados sejam analisados e testes sejam efetuados para se avaliar o quanto de vulnerabilidade daquele controle ainda permanece e/ou o quanto está eficaz para o propósito pelo qual foi estabelecido. No final, deverão ser destacadas no seu relatório as vulnerabilidades encontradas e as oportunidades de melhorias para determinados controles, se for o caso.

Um ponto que merece atenção com relação às vulnerabilidades é o seu **aspecto temporal**, que está relacionado ao momento em que elas possam vir a ocorrer. Uma forma de se facilitar essa descoberta é identificar em quais fases do ciclo de vida da informação (produção, manuseio, transporte, arquivo

e descarte) é mais provável a ocorrência de eventos que podem acarretar danos à integridade, confidencialidade e disponibilidade da informação.

O ideal para se identificarem vulnerabilidades é a utilização concomitante das ferramentas automatizadas, do diagrama e da auditoria, para que o processo de identificação tenha o maior alcance possível, pois as técnicas e ferramentas possuem limitações, como a não detecção da exposição de senhas de acesso pela ferramenta automatizada. Não se deve esquecer-se de recorrer a fontes confiáveis, como os manuais de segurança da informação e as pesquisas.

Algumas perguntas podem ajudar nessa fase, como, por exemplo: A quem poderão interessar essas informações? Por quê? Para quê? A quem poderá interessar a interrupção desse serviço? O que pode ser explorado para prejudicar a confidencialidade, a disponibilidade e a integridade da informação? Quem é a ameaça?

No final dessa etapa, os responsáveis pela identificação dos riscos terão uma relação das vulnerabilidades e possíveis ameaças, a qual permitirá identificar os impactos de sua concretização.

Identificar os impactos

Como foi visto na etapa anterior, as vulnerabilidades, quando exploradas pelas ameaças, podem produzir danos aos negócios e ativos envolvidos, e isso pode ocorrer de forma intencional ou não.

Nessa etapa, devem ser identificados os impactos que as perdas da quebra de requisitos de segurança podem produzir. No caso da norma ISO 27001:2005, os requisitos são: confidencialidade, integridade e disponibilidade.

De modo geral, a perda desses requisitos está diretamente relacionada com os seguintes impactos: divulgação (confidencialidade); modificação (integridade); perda, destruição e interrupção (disponibilidade).

Ao se identificarem os impactos, devem ser consideradas as atividades e os critérios definidos para os requisitos de confidencialidade, integridade e disponibilidade nessas atividades.

Por exemplo, na atividade de negócio de venda pela *web*, o acesso à informação deve ocorrer durante as 24h do dia em todos os dias da semana (disponibilidade); as informações trocadas devem ser mantidas em sigilo e

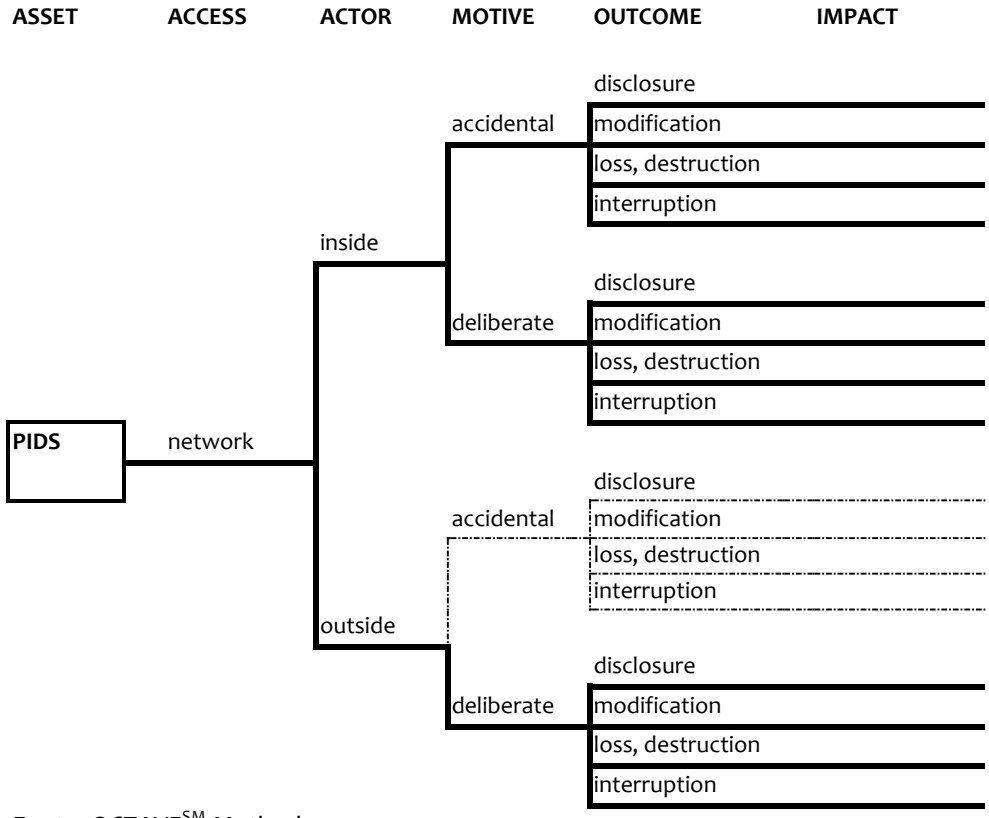
sujeitas às normas de privacidade (confidencialidade); e os registros das transações devem ser mantidos conforme foram gerados (integridade).

Ao se identificarem os impactos, deve-se observar o que poderá ocorrer se determinado requisito for quebrado. No exemplo acima, os impactos identificados poderiam ser: a divulgação indevida das informações dos clientes, a destruição dos registros das transações efetuadas e a interrupção dos serviços de comunicação.

Como impacto de uma falha de *hardware* (ameaça involuntária), pode-se ter: a divulgação de informações confidenciais quando do seu envio para a manutenção externa (confidencialidade); a alteração de parte dos dados processados (integridade), ou a sua destruição (disponibilidade). Como impacto de uma atividade *hacking* (ameaça intencional), pode-se ter: a divulgação e venda de dados de clientes (confidencialidade); a alteração de senhas de acesso aos sistemas (integridade) e a indisponibilidade do *site* (disponibilidade). Como impacto de um alagamento na sala de servidores (ameaça natural), pode-se ter: acesso a informações confidenciais quando da retirada da área alagada (confidencialidade); perda total de equipamentos e informações e indisponibilidade de serviços (disponibilidade).

O método OCTAVE[SM] (*Operational Critical Threat, Asset, and Vulnerability Evaluation*)[28] apresenta um esquema simples, que pode facilitar a identificação de impactos.

[28] *Operational Critical Threat, Asset, and Vulnerability Evaluation* é um método de avaliação de riscos de segurança da informação que foi desenvolvido pelo *Software Engineering Institute* da *Carnegie Mellon University*. Patrocinado pelo *U.S. Department of Defense*, esse método é baseado num conjunto de critérios. Ele define os elementos fundamentais para uma avaliação de riscos de segurança de uma organização.



Fonte: OCTAVE[SM] Method.

Uma técnica que poderá facilitar a identificação dos impactos é a elaboração de um roteiro, do qual constem os seguintes itens:

1- Os ativos por atividade de negócio, seus proprietários, sua criticidade e os requisitos de segurança de cada ativo;
2- As ameaças aos ativos, por categoria: naturais, involuntárias e intencionais;
3- As vulnerabilidades a esses ativos relacionadas com as ameaças;
4- Os possíveis impactos pelas perdas dos requisitos: confidencialidade, integridade e disponibilidade.

Esses impactos devem ser classificados em níveis, como, por exemplo: alto, médio, baixo e desprezível, para serem utilizados na análise dos riscos identificados.

3.3.2 Analisar os riscos

A análise de riscos desenvolve um entendimento sobre os riscos e os seus impactos nas atividades de negócios e ativos envolvidos, no sentido de orientar as melhores estratégias para o tratamento dentro da relação custo-benefício. O objetivo maior é poder segregar os riscos de maiores impactos a fim de se poder eliminar o que puder ser eliminado, e reduzir ou transformar para níveis menores aqueles que não puderem ser eliminados, ou transferi-los para outras partes.

Na fase de analisar os riscos,[29] três fatores são fundamentais: os controles, a probabilidade e as consequências. O fator consequência (impacto) é baseado na valoração do ativo e da sua importância para as atividades de negócios. A sua análise deve levar em consideração os critérios estabelecidos para se avaliarem os impactos, como, por exemplo: financeiro, legal, imagem organizacional, custo do ativo, etc. O fator probabilidade (possibilidade) baseia-se nas ameaças e vulnerabilidades, bem como na sua possível ocorrência. O fator controle tem como base a avaliação da eficácia dos controles existentes, que são materializados em normas, processos, procedimentos e práticas, dentre outros, que compõem todo um arcabouço de uma infraestrutura voltada para a proteção da organização, e em especial para a segurança da informação.

Não se deve esquecer que as análises devem levar em consideração tudo o que foi identificado na etapa de identificação dos riscos, o que, como foi visto, envolveu: a identificação dos ativos, seus proprietários e o valor desses ativos; a identificação das ameaças e a sua relação com as vulnerabilidades, e os impactos que as perdas podem produzir.

É a fase na qual ocorre o estudo detalhado de cada risco e a sua inter-relação com os controles e suas vulnerabilidades. É o que pode ser chamado de estudo do risco propriamente dito.

Um ponto que merece destaque quando tratamos de segurança da informação é que, mesmo considerando o conjunto de critérios para mensurar os impactos, quando a análise é com relação à segurança da informação, em

[29] Recomendamos a releitura do item "métodos de análise e parâmetros de avaliação" do capítulo 2 deste livro, para melhor compreender este tópico.

conformidade com a norma ISO 27001:2005, o fator impacto deve ser analisado com relação aos requisitos de confidencialidade, integridade e disponibilidade, que são requisitos dessa norma. E tal análise leva em consideração o valor do ativo e um valor para o impacto, que pode ser nominal ou em valores absolutos, dependendo do método de análise escolhido (qualitativo, quantitativo, e semiquantitativo); o valor do ativo, e um determinado nível para se identificar a criticidade do impacto.

É com base na combinação desses fatores que as análises são realizadas e é estabelecida a criticidade dos riscos para se elaborar o seu *ranking*. Lembramos mais uma vez que os métodos de análise e os parâmetros de avaliação já devem ter sido estabelecidos quando da escolha da metodologia para o processo de avaliação de riscos, que são informações indispensáveis para o sucesso dessa etapa.

Para uma melhor visualização dessas combinações, deve ser elaborada uma matriz de risco. Abaixo estão apresentados alguns exemplos de matriz de risco.

Matriz de riscos (valores de ativos, possibilidades de ameaças e vulnerabilidades)

Valor do ativo	**Níveis de ameaças**								
	Baixo (B)			**Médio (M)**			**Alto (A)**		
	Níveis de vulnerabilidade								
	B	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Fonte: BS 7799-3:2006

Matriz de riscos (consequências X possibilidade)

	Consequências				
Possibilidade	**Insignificante 1**	**Menor 2**	**Moderado 3**	**Maior 4**	**Catastrófico 5**
A (Frequente)	M	A	A	E	E
B (Provável)	M	M	A	A	E
C (Ocasional)	B	M	A	A	A
D (Remota)	B	B	M	M	A
E (Improvável)	B	B	M	M	A

Fonte: HB 436:2004

Matriz de riscos (ameaças, vulnerabilidade e possibilidade)

Níveis de ameaças	**Baixo (B)**			**Médio (M)**			**Alto (A)**		
Níveis de vulnerabilidade	**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
Valor da possibilidade	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**

Fonte: HB 231:2004

3.3.3 Avaliar os riscos

Na etapa de avaliação dos riscos (*risk evaluate*), é realizada uma comparação entre a classificação de cada risco analisado e o critério de avaliação estabelecido pela organização quando da escolha do método de avaliação.

Como foi visto no capítulo 2, vários parâmetros são utilizados na escolha dos critérios para se avaliarem os riscos, como, por exemplo: financeiros; de imagem organizacional; social e ambiental; pessoal; normativo, etc.

Esses parâmetros são referências escolhidas pela organização e estão relacionados com o tipo de atividade e criticidade do segmento econômico da

organização. Eles servem para se poder dar mais transparência ao processo de segregação dos riscos, bem como tornar o seu tratamento mais objetivo.

Para exemplificar, vamos adotar a matriz de risco a seguir, que identifica os níveis de criticidade dos riscos em quatro categorias: risco extremo, risco alto, risco moderado e risco baixo. Essa matriz faz parte da etapa de análise dos riscos.

Matriz de riscos (consequências X possibilidade)

	Consequências				
Possibilidade	**Insignificante 1**	**Menor 2**	**Moderado 3**	**Maior 4**	**Catastrófico 5**
A (Frequente)	A	A	E	E	E
B (Provável)	M	A	A	E	E
C (Ocasional)	B	M	A	E	E
D (Remota)	B	B	M	A	E
E (Improvável)	B	B	M	A	A

Com base nesta matriz, os riscos devem ser confrontados com os critérios definidos pela organização para a aceitabilidade dos riscos, e poder identificar o que deve ser feito, ou seja, as medidas de tratamento.

Quadro da aceitabilidade dos riscos

Risco extremo (E)	Inaceitável- requer ação corretiva imediata
Risco alto (A)	Inaceitável - requer ação corretiva imediata com atenção específica da direção
Risco moderado (M)	Inaceitável- requer monitoramento, ações de mitigação, e revisão dos controles pelo gerente Aceitável – requer a revisão e autorização do gerente
Risco baixo (B)	Aceitável- requer procedimentos de rotina

Outro padrão que pode ser utilizado para a avaliação é identificar as medidas de tratamento para cada nível de risco (combinação das consequências com as possibilidades), conforme o exemplo abaixo:

Matriz de riscos

CONSEQUÊNCIA	POSSIBILIDADE		
	BAIXA	MÉDIA	ALTA
ALTA	CONSIDERAR	MITIGAR	MITIGAR
MÉDIA	DOCUMENTAR	CONSIDERAR	MITIGAR
BAIXA	DOCUMENTAR	DOCUMENTAR	DOCUMENTAR

Ações de tratamento:
Mitigar: estratégias desenvolvidas para reduzir o risco.
Considerar: meios que a combinação alvo/cenário deve considerar e estratégias mitigadoras que devem ser desenvolvidas em cada caso.
Documentar: não necessita de medidas de tratamento. Deve ser apenas documentado para revisão futura dos riscos avaliados.

A norma ISO 27001:2005 refere-se às etapas da análise e da avaliação dos riscos como uma etapa apenas, que denomina de **analisar e avaliar os riscos**, dividindo-as nas seguintes atividades: 1- avaliar os impactos para o negócio da organização, que podem resultar de falhas de segurança, levando em consideração as consequências de uma perda de confidencialidade, integridade ou disponibilidade dos ativos; 2- Avaliar a probabilidade real da ocorrência de falhas de segurança à luz de ameaças e vulnerabilidades prevalecentes, assim como os impactos associados a esses ativos, e os controles atualmente implementados; 3- Estimar os níveis dos riscos; 4- Determinar se os riscos são aceitáveis ou se requerem tratamento que utilize os critérios para a aceitação dos riscos estabelecidos quando da escolha do método.

Quando se busca a conformidade com essa norma, independentemente do modelo escolhido para o processo de avaliação de riscos, essas atividades devem estar contidas no seu processo, pois a norma não determina que tipo de modelo deve ser utilizado.

Pode-se concluir, portanto, que a avaliação do risco é a base para que sejam identificadas as ações de tratamento dos riscos, que é a etapa seguinte do gerenciamento de riscos.

3.3.4 Análise de riscos X Avaliação de riscos

Existe determinada confusão entre os conceitos de avaliação e análise de riscos, e pode ser comum encontrar alguns autores se referindo ao processo de avaliação de riscos atribuindo-lhe o nome de análise de riscos. Compreender essa diferença é fundamental quando estudamos os riscos.

Por mais que desejemos finalizar essa discussão, algumas dúvidas poderão surgir sobre essa questão, transpondo o campo da semântica. Entretanto, na prática, tais concepções necessitam estar bem delimitadas, a fim de que não existam dúvidas para os aplicadores da gestão dos riscos sobre o processo de avaliação dos mesmos.

Na pesquisa realizada, foi verificado o emprego dos termos avaliação de riscos e análise de riscos com o mesmo significado. Eles possuem significados diferentes, constituem etapas específicas do processo de gestão de riscos, e não podem ser utilizados como expressões sinônimas.

Essa diferenciação já é percebida no significado das palavras análise e avaliação, que, segundo o dicionário (Houaiss, 2005) significam:

> **Análise**: ato ou efeito de analisar-se; separação de um todo em seus elementos ou partes componentes; estudo pormenorizado de cada parte de um todo, para conhecer sua natureza, suas funções, relações, causas, etc.; exame, processo ou método com que se descreve, caracteriza e compreende algo, para proporcionar uma avaliação crítica do mesmo.
>
> **Avaliação**: ato ou efeito de avaliar-se; apreciação ou conjectura sobre condições, extensão, intensidade, qualidade de algo; verificação que objetiva determinar a competência, o progresso, etc. de um profissional, aluno, etc.

Como se pode ver, a avaliação é mais ampla do que a análise, mais restrita. Isso também ocorre quando estudamos os riscos.

A norma ISO/IEC Guide 73 emprega o termo avaliação de riscos (*risk assessment*) para se referir ao processo geral de análise e de avaliação de riscos (*risk evaluation*), e o termo análise de riscos refere-se às etapas de identificar as fontes de riscos e estimá-los.

A norma AS/NZS 4360:2004 emprega o termo avaliação de riscos (*risk assessment*) para referir-se ao processo geral de identificação, análise e avaliação de riscos (*risk evaluation*), e o termo análise de riscos para se referir ao processo sistemático para entender a natureza e inferir sobre o nível de risco.

Dessa forma, ao nos referirmos à avaliação de riscos (*risk assessment*), devemos compreender que é o processo geral, mais amplo, e à análise de riscos como o processo específico de análise para cada risco identificado.

Outra questão que merece destaque é com relação ao termo *evaluation,*[30] que significa avaliação. Contudo, ao empregarmos a expressão avaliação de riscos (*risk evaluation*), estaremos a nos referir ao processo de comparação do risco estimado com determinado critério de risco, a fim de determinar a sua relevância. Essa avaliação pontual é utilizada para as ações de tratamento do risco. Ela é uma etapa do processo maior de avaliação (*assessment*).

Nesse sentido, podemos concluir que, pelos padrões internacionais (ISO, BSI e AS/NZS), a avaliação de riscos é um processo geral, que possui como uma de suas etapas a análise do risco, a fim de que ele possa ser comparado com determinados critérios para se estabelecer um nível de relevância, no sentido de ajudar na tomada de decisão sobre tal risco. Essa comparação para o estabelecimento da criticidade do risco para tratamento é chamada de avaliação de riscos (*risk evaluation*), e deve ser entendida como uma avaliação pontual, ou seja, para aquele tipo de risco.[31]

---

[30] Neste trabalho, empregaremos o termo em inglês "*risk evaluation*" para nos referirmos à avaliação do risco (mais pontual, para cada risco), e a expressão "*risk assesment*" para o processo de avaliação de riscos (mais amplo).

[31] No nosso trabalho, quando nos referirmos às definições e metodologias de autores pesquisados, utilizaremos as expressões desses autores, preservando a fonte e respeitando seus entendimentos; contudo, adotaremos como referência o padrão internacional das normas ISO, BSI e AS/NZS.

Considerações às normas ABNT ISO/IEC Guia 73:2005, NBR ISO/IEC 27002:2005, NBR ISO/IEC 27001:2006, e NBR ISO/IEC 27005:2008, com relação às expressões análise/avaliação de riscos, análise de riscos e avaliação de riscos

Essas normas da ABNT, quando se referem à avaliação de riscos (*risk assessment*), utilizam a expressão **análise/avaliação de riscos** para se referirem ao processo geral de análise e avaliação de riscos, e os termos análise de riscos e avaliação de riscos para se referirem às etapas específicas desse macroprocesso: a análise de riscos como o uso sistemático de informações para identificar fontes e estimar o risco; e a avaliação de riscos (*risk evaluation*) como o processo de comparar o risco estimado com os critérios predefinidos para determinar a importância do risco.

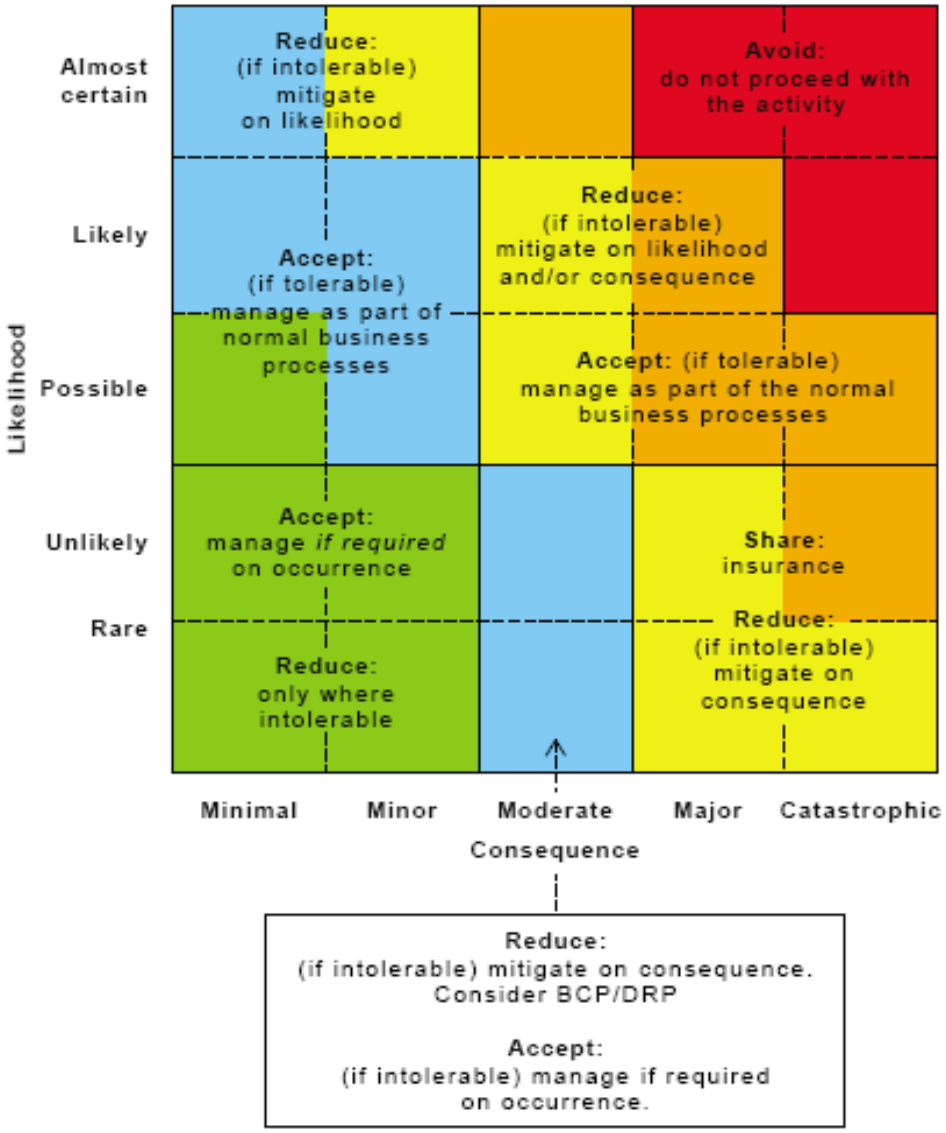
Elas constituem a versão brasileira (em português) do padrão ISO, e são elaboradas com base na versão original que é em inglês. Daí, quando da tradução do significado estrito da palavra, podem-se encontrar alguns termos com o mesmo significado, como é o caso dos termos em inglês *assessment* e *evaluation*, que significam avaliação. Contudo, eles, quando utilizados no contexto do gerenciamento de riscos, representam atividades distintas.

Dessa forma, ao nos referirmos a essas expressões, neste livro, utilizaremos os termos das normas ISO/IEC Guide 73:2002, da AS/NZS 4360:2004 e da BSI 7799-3:2006. Já as normas NBR ISO/IEC 27002:2005, NBR ISO/IEC 27001:2006, e NBR ISO/IEC 27005:2008 são utilizadas como referências específicas para o sistema de gestão de segurança da informação, no contexto deste livro.

3.4 Tratamento de riscos

Ao se concluirmos o processo de avaliação de riscos, temos uma listagem com todos os riscos por nível de criticidade, bem como orientações genéricas para o que devemos fazer.

A figura abaixo exemplifica como pode ser orientada a escolha da melhor estratégia para o tratamento dos riscos:



Fonte: HB 292:2006

O detalhamento dessas ações são atividades específicas de uma nova etapa denominada tratamento de riscos, que, segundo a ISO Guide 73:2002, é o processo de seleção e implementação de medidas para modificar o risco.

O tratamento dos riscos tem como objetivos eliminar os riscos que podem ser eliminados; transformar (ou reduzir) o nível dos riscos que não podem ser eliminados para um nível menor e com o mínimo de dano para a organização; transferir o risco (ou parte dele) que não pode ser tratado, e evitar os riscos que podem ser evitados.

A eliminação, o monitoramento e a transformação dos riscos alcançam a maioria das ações de tratamento dos riscos. Essas medidas são lastreadas nos processos que envolvem as medidas para reduzir a probabilidade e as consequências negativas relacionadas com os riscos.

As ações para evitar o risco, como o próprio nome já sugere, são todas as medidas adotadas para evitar que um risco venha a ser concretizado, e essas medidas estão representadas nas políticas e procedimentos da organização.

A transferência do risco é a divisão com outra parte do peso de perdas de um risco. É materializada nos contratos de terceirização e nas apólices de seguro. Nas apólices de seguro, por exemplo, o peso da perda é minimizado com o pagamento do prêmio do seguro, que é de valor bem menor do que os ativos envolvidos.

A retenção do risco é a aceitação da carga da perda de um risco específico. Geralmente é feita com os riscos de pequeno impacto.

Dessa forma, como foi visto acima, pode-se afirmar que o tratamento dos riscos compreende as ações para evitar, otimizar, transferir e/ou compartilhar e reter o risco.

As normas ISO Guide 73:2002, AS/NZS 4360:2004, e BS 7799-3:2006 referem-se a essas ações, cujo foco principal é eliminar ou reduzir a probabilidade e as consequências de um risco.

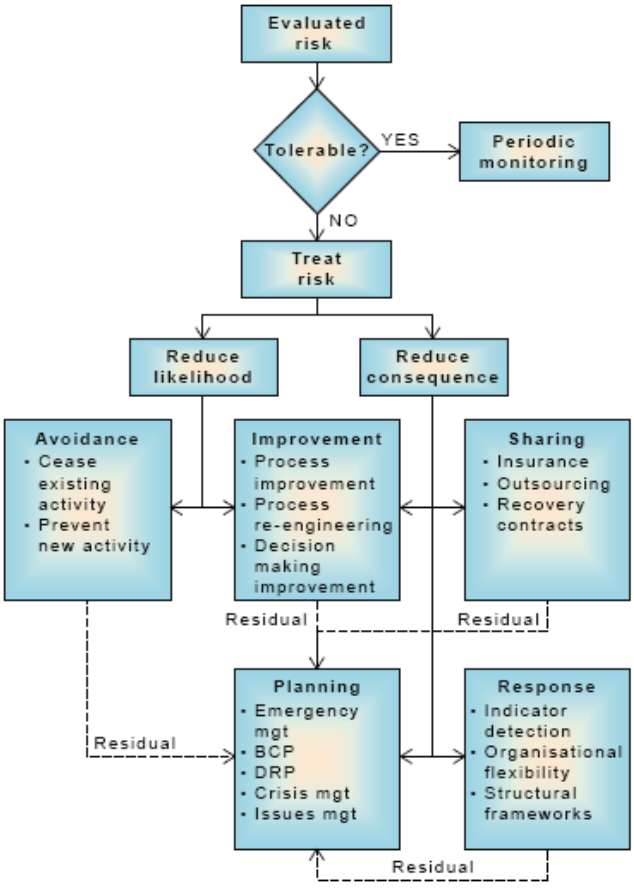
A norma ISO 27001:2005 estabelece que as opções de tratamento dos riscos devem incluir: 1- aplicar os controles apropriados; 2- aceitar os riscos consciente e objetivamente, desde que satisfaçam claramente as políticas da organização e os critérios de aceitação dos riscos; 3- evitar os riscos, e 4- transferir os riscos associados ao negócio a outras partes, por exemplo, seguradoras e fornecedores.

O HB 231:2004 apresenta que as opções para o tratamento dos riscos devem incluir: 1- evitar os riscos; 2- reduzir as possibilidades; 3- reduzir as consequências; 4- transferir os riscos, e 5- reter os riscos.

O HB 436:2004 apresenta um roteiro para se estabelecerem as opções de tratamento, que possui as seguintes etapas: 1- Revisar as causas e os controles existentes; 2- Estabelecer os objetivos do tratamento; 3- Detalhar as medidas de tratamento; 4- Revisar as medidas escolhidas; 5- Comunicar e implementar.

Conforme se pode verificar, todos os padrões acima focam as atividades de tratamento com o objetivo maior de reduzir ou transformar, transferir e/ou compartilhar, e evitar os riscos, para que a organização possa vir a desenvolver as suas atividades de negócios em um ambiente de riscos gerenciáveis.

A figura a seguir exemplifica algumas opções de tratamento:



Fonte: HB 292:2006

Como foi visto em capítulo anterior, na escolha das opções de tratamento para os riscos, devemos atentar para dois aspectos: a prevenção e a reação. Ratificamos, assim, que devemos observar o antes, o durante e o depois, para a escolha da melhor opção para cada uma dessas fases.

Um ponto que merece atenção na escolha da opção de tratamento é com relação aos riscos de baixa probabilidade e alto impacto. Às vezes, esses riscos não recebem qualquer atenção para tratamento e são praticamente descartados ou aceitos. Geralmente esses riscos são negligenciados, mesmo quando possuem o poder de destruir o valor da empresa. Nesses casos, entendemos que o estabelecimento de cenários predefinidos é oportuno para se determinarem as ações preliminares de resposta. Não devemos esquecer, também, que algumas ações de prevenção são fundamentais, principalmente quando se consideram os riscos de origem nos fenômenos da natureza, por exemplo.

Outra questão diz respeito à relação custo-benefício da medida escolhida. Essa análise geralmente é financeira, para não se ter uma escolha cujo custo total seja superior ao impacto calculado para o risco em questão. Entretanto, alguns pontos podem ser levados em consideração, como a aceitabilidade da ação frente ao segmento de mercado, à tecnologia empregada e à praticidade da medida adotada.

Todas essas ações são descritas no plano de tratamento de riscos, documento que consolida todas as ações de tratamento e a sua forma de implementação, identificando as responsabilidades e estabelecendo os prazos, recursos, mecanismos de avaliação e controle, dentre outras.

Essas ações de tratamento são materializadas em controles. Cada controle deve ser estabelecido com uma finalidade específica, que é denominada objetivo de controle.

Em se tratando de controle, o grande desafio é identificar o controle ou o sistema de controle ideal. Nesse sentido, o padrão ISO é um referencial internacional bastante aceito. Para tanto, devemos atentar para as normas ISO 27002:2005 (incluída na família das normas ISO 27000) e 27001:2005. A primeira apresenta diretrizes para a implementação de um sistema de gestão de segurança da informação, e a segunda estabelece os requisitos obrigatórios para esse sistema e os seus controles mínimos.

É lógico que não existe a obrigatoriedade de se certificar na norma ISO 27001:2005, mas, sem dúvida, que ao se alinhar com tais requisitos a organização possuirá um sistema de gestão de segurança da informação (ISMS) dentro de padrões internacionalmente reconhecidos e aceitos.

3.5 Revisão e monitoramento

Como em todo processo de gestão, o gerenciamento de riscos também precisa ser monitorado e revisto. O monitoramento deve ser feito com base em vigilância cotidiana da *performance* do sistema, uma vez que os cenários são dinâmicos e susceptíveis às mudanças. A revisão desse processo deve ocorrer periodicamente a respeito de fatos presentes e com um foco bem específico. Ambas as atividades são essenciais para uma boa gestão dos riscos.

O monitoramento e a revisão devem estar atentos para as mudanças no ambiente da organização, para os riscos e seus níveis de criticidade e para as medidas de tratamento, com priorização para os riscos de impacto elevado, especialmente nas atividades críticas de negócios, em que os ativos envolvidos sejam estratégicos e possuam um custo elevado de reposição.

Essas atividades podem ser executadas: por meio da medição de parâmetros definidos, nas rotinas das atividades cotidianas; em atividades específicas, que demandem mais atenção e preocupação com a manutenção de um nível mínimo de *performance* para determinada atividade; mediante a realização de auditorias, que são excelentes ferramentas para o exame de sistemas.

Todo e qualquer incidente de segurança, seja ele intencional, seja acidental, deve ser analisado, mesmo que as ações específicas de resposta e recuperação tenham sido eficazes, para que se possa avaliar se tais medidas poderiam ter sido mais otimizadas, e até que nível de impacto elas seriam eficazes. Um erro comum é não realizar uma avaliação crítica das ações realizadas, o que, em alguns casos, pode abrir fendas de vulnerabilidades, em se considerando que tais medidas poderiam não manter o padrão de resposta desejado se tal evento fosse de uma gravidade um pouco maior.

Outro ponto importante, e que pode passar despercebido, é o fato de que se procura estudar casos ocorridos em outras organizações, e avaliar como a organização se comportaria frente a um evento semelhante. Com isso se estará fomentando um processo de aprendizagem e semeando a cultura de uma gestão arrojada sobre os riscos, ao se tentar entender e estudar possíveis eventos futuros, preparando-se para quaisquer eventualidades.

3.6 Ferramentas utilizadas para a gestão de riscos

A gestão de riscos é um processo complexo, e a conclusão de todas as suas fases pode demandar um bom período de tempo. Dessa forma, a utilização de ferramentas é indispensável para tornar esse processo cada vez mais otimizado e bem mais fácil de ser realizado.

As ferramentas utilizadas nesse processo variam de simples planilhas, tabelas, questionários, até programas específicos para atividades pontuais ou para todo o processo. De acordo com essa filosofia, este capítulo trata sobre alguns tipos de ferramentas utilizadas na gestão de riscos.[32]

Checklist

O *checklist* é uma ferramenta bastante utilizada para a checagem de aspectos referentes à identificação de ameaças e vulnerabilidades. É uma ferramenta importante na avaliação da criticidade das atividades de negócios corporativos face às suas ameaças e vulnerabilidades, e pode ser facilmente utilizada pelo pessoal de cada unidade de negócio e pelos proprietários dos ativos. A sua utilização requer a verificação "in loco".

Análise GAP

A análise GAP[33] (*Gap analysis*) é um exame de auditoria que objetiva verificar a conformidade com as políticas, normas e procedimentos relacionados com a segurança da informação. É uma comparação da situação

[32] O objetivo deste capítulo não é optar por tal ou qual ferramenta, mas comentar e apresentar algumas ferramentas que se têm apresentado como eficazes no processo de gestão de riscos.
[33] O termo Gap vem do inglês e significa fenda, abertura, brecha, intervalo. Análise GAP é uma análise que objetiva fechar a brecha da segurança. Esse é o significado que desejamos ao empregar o termo "Análise GAP".

atual com o padrão estabelecido. É um exame superficial, uma vez que apenas identifica se os controles estão ou não alinhados com o padrão estabelecido.

Serve como ponto referencial para avaliar a extensão e complexidade do processo de avaliação de riscos a ser implementado. É uma excelente ferramenta para o planejamento e definição do escopo da avaliação dos riscos e do sistema de gestão a ser estruturado.

A análise GAP pode ser realizada com base nos controles aplicáveis e em níveis de referência (maturidade, por exemplo). A realizada com base nos controles aplicáveis é sobre as normas de referência, verificando os itens dessas normas e comparando-os com os controles existentes na organização. Na análise baseada em níveis de controle, é realizado o exame sobre uma classificação de referência, no qual é verificado em qual estágio de controle se encontra a organização em determinado setor, área, atividade, etc.

Ferramentas GGRS1, GGRS2 e GGRS3

As planilhas também são bastante utilizadas no processo de gestão de riscos. Várias são as suas utilizações, como, por exemplo: identificação de funções críticas de negócios; análise de vulnerabilidades e riscos; análise de impacto nos negócios; desenvolvimento de estratégias, etc.

O Guia de gerenciamento de riscos de segurança da Microsoft (Microsoft, 2005) apresenta as ferramentas GGRS1, GGRS2 e GGRS3, que são planilhas utilizadas para facilitar o processo de análise e avaliação de riscos.

A **ferramenta GGRS1** é uma planilha utilizada para a coleta de dados, coleta essa que é detalhada pelo nome do ativo e sua classificação, sendo completada com a camada de defesa em profundidade, suas ameaças, vulnerabilidades, o nível de exposição do ativo, os controles atuais, as probabilidades e os possíveis novos controles. A sua estrutura está representada na figura abaixo.

Modelo de coleta de dados

Identifique os ativos pelos quais o seu grupo é responsável pelo desenvolvimento, gerenciamento, suporte ou manutenção.

Nome do ativo	Classificação do ativo (impacto comercial alto, médio ou baixo)
1.	

Complete os seguintes dados para cada ativo:

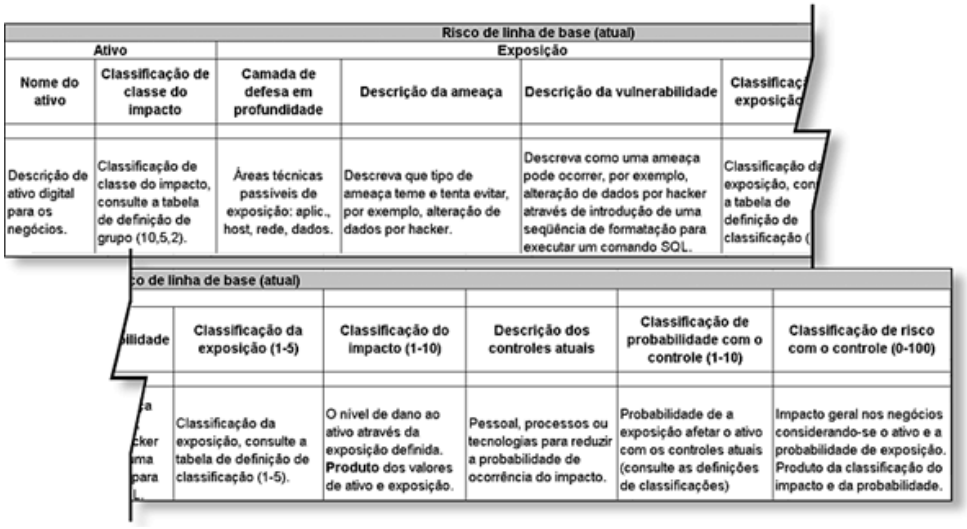
Camada de defesa em profundidade	O que você teme ou tenta evitar: (ameaças)	Como isso pode ocorrer: (vulnerabilidades)	Nível de exposição (A, M, B)	**Descrição dos controles atuais**	Probabilidades (A, M, B)	**Problemas do controle, possíveis novos controles**
Física						
Aplicativo						
Host						
Rede						
Dados						

A **ferramenta GGRS2** é composta de mais de uma planilha e destina-se a mostrar o nível de risco resumido. Essa ferramenta apresenta a descrição de cada ativo avaliado e a sua classe, a camada de defesa em profundidade vulnerável à ameaça, a ameaça, suas vulnerabilidades, o nível de exposição e a classificação do impacto. A sua estrutura está representada na figura a seguir.

Informações obtidas durante o processo de coleta de dados							
Ativo				Exposição			
Data da identificação	Nome/descr. do ativo	Classe do ativo	Camadas de defesa em profundidade completa aplicáveis	Descrição da ameaça	Descrição da vulnerabilidade	Nível de exposição (A, M, B)	Classificação do impacto (A, M, B)

Essa ferramenta ainda apresenta as planilhas de classe de ativo e nível de exposição, assim como a planilha de impacto e probabilidade.

A **ferramenta GGRS3** é composta de mais de uma planilha e destina-se a apresentar a lista detalhada dos risco. Para isso, apresenta planilhas de classificação da exposição da disponibilidade, confidencialidade e integridade; para determinar valores de impacto; de avaliação de vulnerabilidade; para atribuir valores à probabilidade, e de avaliação da eficácia e controle atual. A planilha da lista detalhada dos riscos está representada na figura abaixo.



Risco de linha de base (atual)						
Ativo		Exposição				
Nome do ativo	Classificação de classe do impacto	Camada de defesa em profundidade	Descrição da ameaça	Descrição da vulnerabilidade	Classificaç exposiçã	
Descrição de ativo digital para os negócios.	Classificação de classe do impacto, consulte a tabela de definição de grupo (10,5,2).	Áreas técnicas passíveis de exposição: aplic., host, rede, dados.	Descreva que tipo de ameaça teme e tenta evitar, por exemplo, alteração de dados por hacker.	Descreva como uma ameaça pode ocorrer, por exemplo, alteração de dados por hacker através de introdução de uma seqüência de formatação para executar um comando SQL.	Classificação d exposição, con a tabela de definição de classificação (	

co de linha de base (atual)					
ilidade	Classificação da exposição (1-5)	Classificação do impacto (1-10)	Descrição dos controles atuais	Classificação de probabilidade com o controle (1-10)	Classificação de risco com o controle (0-100)
ca cker uma para L.	Classificação da exposição, consulte a tabela de definição de classificação (1-5).	O nível de dano ao ativo através da exposição definida. **Produto** dos valores de ativo e exposição.	Pessoal, processos ou tecnologias para reduzir a probabilidade de ocorrência do impacto.	Probabilidade de a exposição afetar o ativo com os controles atuais (consulte as definições de classificações)	Impacto geral nos negócios considerando-se o ativo e a probabilidade de exposição. Produto da classificação do impacto e da probabilidade.

Risk Vision

A ferramenta *Risk Vision*[34] é uma ferramenta de TI com o processo de gestão de riscos corporativos. O processo de GRC utiliza o método Brasiliano de análise de riscos. É uma ferramenta que possibilita que se avaliem e gerenciem as incertezas como forma de criação de vantagem competitiva.

Essa ferramenta alinha estratégia, processos, pessoas, tecnologia e conhecimentos para a análise de riscos. Nesse processo de análise, os riscos não são tratados como fatos isolados, mas por meio de uma metodologia de gestão integrada que prioriza os riscos de maior importância e relevância para a empresa, evitando que não sejam devidamente gerenciados, ou, eventualmente, que os riscos menos importantes sejam controlados de modo excessivo.

A sua grande vantagem é a possibilidade de utilizar o método qualitativo e quantitativo de avaliação de riscos conjuntamente, pois os transforma num mesmo parâmetro, obtendo ganho de tempo e eficiência no processo como um todo.

[34] Mais informações podem ser obtidas no endereço: http//www.sicurezza.com.br

RA2 art of risk

A ferramenta *RA2 art of risk*[35] é um *software* direcionado para o desenho e a implementação de um sistema de gestão de segurança da informação (ISMS), em conformidade com a norma ISO 27001:2005.

Essa ferramenta ajuda a definir o escopo e requisitos de negócios, políticas e objetivos para o ISMS; a desenvolver o inventário dos ativos; a conduzir o processo de avaliação de riscos; nas decisões das opções de tratamento; na escolha dos controles apropriados e em conformidade com os controles previstos no anexo A da norma ISO 27001:2005, e na seleção de toda a documentação necessária para o ISMS.

Ela traz referenciais de criticidade para a avaliação de ativos, vulnerabilidades e ameaças, que podem ser utilizados em vários níveis, além de construir a declaração de aplicabilidade.[36]

É uma ferramenta de fácil manuseio e praticidade e tem sido muito bem aceita pela comunidade de segurança da informação.

Módulo Risk Manager

A ferramenta *Módulo Risk Manager*[37] é um *software* implementador de processos que alcançam governança, riscos e conformidade com os diversos padrões e regulamentações de mercado e de governança em tecnologia da informação, de forma a facilitar a priorização das ações e os recursos envolvidos.

É uma ferramenta de grande amplitude, pois consegue atender aos requisitos das principais normas de controle, tais como: Sarbanes-Oxley (SOX), PCI-DSS, ISO 27001:2005, COBIT, Basiléia II, FISAP, etc.

Dentre os seus benefícios destacam-se: a criação de um *scorecard* para os riscos com uma visão relacionada com o negócio, o que permite alocar os investimentos de acordo com a criticidade de cada ativo; mapeamento da evolução dos riscos; visão georreferenciada dos riscos; auditorias mais

[35] Mais informações podem ser obtidas no endereço:
http://www.itgovernance.co.uk/products/165

[36] A Declaração de Aplicabilidade (Statement of Applicability) é uma exigência para a certificação de conformidade dos sistemas de gestão de segurança da informação com a norma ISO 27001. É uma declaração documentada que descreve os objetivos de controle e os controles que são aplicáveis ao sistema, como também a justificativa daqueles controles excluídos.

[37] Mais informações podem ser obtidas no endereço: http://www.modulo.com.br

produtivas; apoio à implementação dos requisitos de certificação para SOX, PCI-DSS, ISO 27002, ISO 27001, BS 25999, COBIT, Basiléia II e FISAP; gestão integrada para os riscos da organização; ampla integração, etc.

É uma ferramenta bastante conceituada, que tem apresentado excelentes resultados para quem a utiliza, vindo a ser reconhecida como uma das mais completas com relação às regulamentações específicas do segmento de tecnologia da informação.

Microsoft Security Assessment Tool

A Ferramenta Microsoft Security Assessment Tool[38] (MSAT) é um *software* de avaliação de riscos que fornece informações e recomendações sobre as boas práticas para a segurança da informação em organizações de médio porte que tenham entre 50 e 1.500 desktop.

Essa ferramenta utiliza o conceito de defesa em profundidade, ou seja, oferece orientações para a implementação de controles nas seguintes camadas: infraestrutura, aplicativos, operações e pessoal. No final, fornece um relatório dos resultados com duas avaliações: uma com o perfil de risco da empresa, e outra com a avaliação da defesa em profundidade.

É uma ferramenta fácil de ser utilizada e é uma opção para organizações com recursos limitados para investimentos em segurança da informação.

[38] Mais informações no site: http://technet.microsoft.com/pt-br/security/cc297183.aspx

4. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

O processo de gestão de riscos envolve um conjunto de atividades baseadas em critérios que focam os principais riscos que afetam uma organização. Esses critérios são requisitos e/ou princípios que uma organização adota para estabelecer um padrão de conformidade com o nível de *performance* dos serviços e/ou bens ofertados por ela, frente às exigências do mercado.

Com relação à segurança, esse processo de gestão de riscos deve estar alinhado com a filosofia do negócio, para que se possa desenvolver um modelo de sistema de segurança adequado às atividades do segmento de negócio da organização.

Um sistema de segurança normalmente se sustenta em 3 pilares: normas e procedimentos, recursos humanos e tecnologia. São pilares fundamentais para quaisquer sistemas de proteção. Para a comunidade da segurança, essa questão é tratada pela segurança orgânica, que "compreende o conjunto de medidas passivas que visam prevenir e obstruir ações adversas de elementos ou grupos de qualquer natureza, dirigidos contra a instituição" (Dantas, 2003:88).

De maneira geral, um sistema de segurança compõe todo um arcabouço de políticas, procedimentos, recursos humanos, tecnologia de suporte e infraestrutura necessários ao funcionamento das atividades voltadas para a segurança de uma organização.

Um sistema de informações é constituído por um conjunto de elementos ou componentes inter-relacionados que coletam, manipulam e disseminam os dados e a informação para as atividades de negócios. Ele é composto de *hardware*, *software*, bancos de dados, telecomunicações, pessoas e procedimentos, que formam a infraestrutura tecnológica de uma organização.

Com relação à segurança da informação, o objetivo principal de um sistema é manter a informação segura dentro dos requisitos de segurança definidos por ela, ou pelo padrão adotado. Sem se identificarem os requisitos de segurança, não há como se falar em segurança, uma vez que não se sabe para que se deva estar protegido.

Dentre as fontes de requisitos, três são fundamentais: a primeira é com relação à legislação em vigor, que é o marco regulatório e engloba todo um aparato normativo, desde as questões constitucionais até os procedimentos mais singelos de uma atividade de trabalho; a segunda fonte alcança todo um conjunto de princípios, valores, objetivos e requisitos de negócios, que definem as diretrizes dos negócios corporativos; e a terceira é oriunda do processo de avaliação de riscos, que apresenta para a organização uma relação dos principais riscos, sua criticidade, impactos e danos que podem provocar.

Identificadas as fontes e estabelecidos os requisitos, o sistema de segurança deve ser estabelecido com base em controles que possam satisfazer a essas condições. Um controle deve ser estabelecido com uma finalidade específica, que, como já foi visto, se denomina objetivo de controle, que é o motivo pelo qual ele foi criado.

As fontes, os requisitos, os controles, dentre outros fatores, são verdadeiros desafios para se desenhar um sistema de segurança, e esse desafio conduz à adoção de um padrão de segurança reconhecido e aceito pela sua praticidade e eficácia, que possa ser avaliado de acordo com os requisitos estabelecidos, para que se possa alcançar um nível de confiabilidade que, além de garantir a segurança de seus funcionários, clientes, fornecedores e acionistas, projete a imagem de uma organização segura para o ambiente de negócios, proporcionando-lhe uma verdadeira vantagem competitiva.

Um sistema de segurança pode ser criado, ou pode ser simplesmente adotado de um modelo conhecido. Nesse sentido, o padrão ISO demanda uma atenção específica.

4.1 Sistema de gestão de segurança da informação ISO 27001:2005

Em se tratando de Sistemas de Gestão de Segurança da Informação (ISMS[39]), o padrão ISO é um referencial internacionalmente aceito, e disciplinado nas normas ISO 27002 e 27001.

[39] Information Security Management System.

A norma ISO 27002:2005 estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Essa norma possui uma seção introdutória sobre o processo de avaliação e tratamento de riscos e está dividida em 11 seções específicas, que são: política de segurança da informação; organização da segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de sistemas de informação; gestão de incidentes de segurança da informação; gestão da continuidade do negócio, e conformidade.

Essas seções totalizam 39 categorias principais de segurança, e cada categoria contém um objetivo de controle e um ou mais controles que podem ser aplicados, bem como algumas diretrizes e informações adicionais para a sua implementação.

Por exemplo, a seção 5 da norma ISO 27002:2005 tem como **objetivo**: prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. E apresenta os seguintes **controles**: no item 5.1.1 Documento da política de segurança da informação - convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes; no item 5.1.2 Revisão (análise crítica) da política de segurança da informação- convém que a política de segurança da informação seja revisada (analisada criticamente) a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

A norma ISO 27001:2005 especifica os requisitos para estabelecer, implementar, operar, monitorar, revisar (analisar criticamente), manter e melhorar um ISMS documentado dentro do contexto dos riscos de negócios globais da organização. E especifica, também, os requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes.

Ela está dividida em 8 seções, que são: 1- Objetivo; 2- Referência normativa; 3 -Termos e definições; 4- Sistema de gestão de segurança da informação; 5- Responsabilidade da direção; 6- Auditorias internas do ISMS; 7- Revisão (análise crítica) do ISMS pela direção, e 8- Melhoria do ISMS.

Essa norma ainda possui um anexo normativo, denominado **anexo A**, que lista os objetivos de controle e os controles mínimos que um ISMS deve possuir. Esses controles não são exaustivos, podendo a organização estabelecer outros controles adicionais. Esses objetivos de controle e controles derivam da norma ISO 27002:2005 e são alinhados com os listados nas seções 5 a 15 da referida norma.

A diferença entre as normas ISO 27002 e 27001 é que a primeira apenas apresenta diretrizes gerais para um ISMS, ou seja, um guia de boas práticas. A segunda é que estabelece os requisitos obrigatórios para um ISMS. É justamente com base na segunda que é concedida a certificação de conformidade com o padrão ISO de segurança da informação. Na prática, utiliza-se a primeira para se obter uma orientação para um ISMS, e a segunda para obter a certificação de conformidade, pois é essa norma (ISO 27001:2005) que é utilizada nas auditorias de certificação.

Os principais benefícios de se possuir um ISMS em conformidade com a norma ISO 27001:2005 são: ter um sistema de segurança baseado em um padrão internacionalmente aceito; abordagem por processo dentro do modelo PDCA; abordagem sistêmica para a gestão; estabelecimento de políticas específicas para a segurança da informação; controles definidos com base nos principais riscos e suas interferências no ambiente de negócios; identificação de ativos e proprietários com responsabilidades específicas para com a segurança da informação; conscientização e treinamento em segurança da informação; realização de ações preventivas, corretivas e de auditorias; revisão (análise crítica) pela direção, e melhoria contínua, dentre outros.

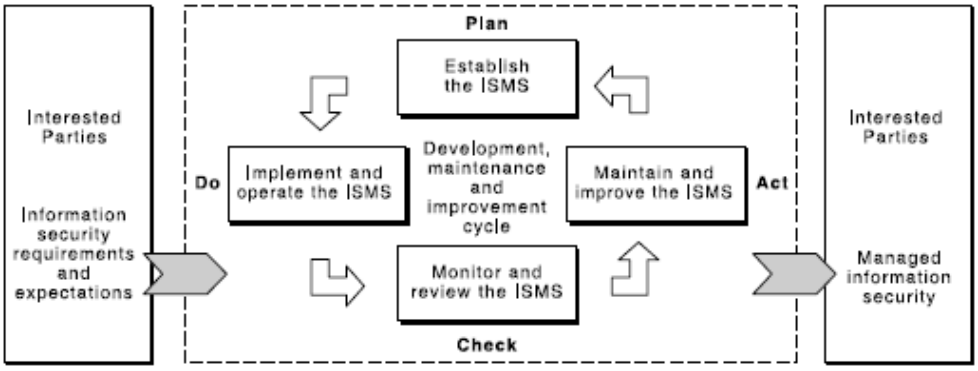
Quando se trata de ISMS em conformidade com a norma ISO 27001:2005, dois aspectos devem ser levados em consideração: um diz respeito ao sistema em si, e o outro tem relação com seus controles.

A norma ISO 27001:2005 define um sistema de gestão de segurança da informação (ISMS) como:

"A parte do sistema de gestão global, baseado na abordagem de riscos ao negócio, para estabelecer, implementar, operar, monitorar, revisar (analisar criticamente), manter e melhorar a segurança da informação."

Esse sistema inclui a estrutura organizacional, as políticas, as atividades de planejamento, as responsabilidades, práticas, procedimentos, processos e recursos.

Essa norma promove a adoção de uma abordagem por processo para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar o ISMS, e adota o modelo PDCA[40] para estruturar todos os processos desse sistema. A figura abaixo representa a abordagem por processo e o sistema PDCA:



Fonte: ISO 27001:2005

O quadro abaixo resume as fases desse modelo:

Plan (planejar) (estabelecer o ISMS)	Estabelecer a política, objetivos, processos e procedimentos do ISMS relevantes para a gestão de riscos e a melhoria da segurança da informação, para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) (implementar e operar o ISMS)	Implementar e operar a política, controles, processos e procedimentos do ISMS.
Check (Checar) (monitorar e revisar o ISMS)	Avaliar e, quando aplicável, medir o desempenho de um processo frente a política, objetivos e experiência prática do ISMS, assim como apresentar os resultados para sua revisão pela direção.

[40] Plan-Do-Check-Act (PDCA).

Act (Agir) (manter e melhorar o ISMS)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do ISMS e da revisão pela direção ou outra informação pertinente, para alcançar a melhoria contínua do ISMS.

Fonte: ISO 27001:2005

Como se pode ver, para que seja configurado um ISMS em conformidade com a norma ISO 27001:2005, faz-se necessário que a organização atenda a todos os requisitos das seções 4 a 8. Quando se pretende a conformidade com essa norma, não é admitida a exclusão de quaisquer dos requisitos especificados nessas seções (4 a 8).

A seção 4 trata do sistema em si. Nela são apresentados todos os requisitos para as fases específicas do modelo PDCA, que são: estabelecer o ISMS (4.2.1), implementar e operar o ISMS (4.2.2), monitorar e revisar o ISMS (4.2.3), e manter e melhorar o ISMS (4.2.4). Inclui, ainda, os requisitos de documentação, e dos controles dos documentos e dos registros. A seção 5 trata das responsabilidades da direção e da gestão de recursos, com itens específicos para a provisão dos recursos e dos treinamentos, conscientização e competência. A seção 6 dispõe sobre as auditorias internas. A seção 7 aborda a revisão (análise crítica) do sistema pela direção. A melhoria contínua é o tema da seção 8, que estabelece os requisitos para as ações corretivas e preventivas.

São vários os detalhes de cada seção, que inclui os requisitos para: definição do escopo e limites do ISMS e da política de segurança da informação, da definição da abordagem do processo de avaliação de riscos, identificar, analisar e avaliar os riscos, identificar e avaliar as opções de tratamento dos riscos, selecionar os objetivos de controle e os controles, aprovar os riscos residuais, obter autorização para implementar e operar o sistema e preparar a declaração de aplicabilidade; formulação e implementação do plano de tratamento, dos controles e da aferição de sua eficácia, da implementação dos programas de conscientização e treinamento, gerenciamento das operações e recursos do sistema, procedimentos de

monitoramento, implementação de melhorias, responsabilidades para conduzir uma revisão e suas entradas e saídas, dentre outros.

4.2 Os controles do ISMS

Como já foi visto, a norma ISO 27001:2005 possui um anexo A, normativo, que lista os objetivos de controle e os controles.[41] Em um ISMS em conformidade com essa norma, tais objetivos de controle e os controles fazem parte de um documento denominado declaração de aplicabilidade, conhecido como SoA (Statement of Applicability).

Nela, a exclusão de qualquer controle deve ser devidamente justificada. Observa-se, no entanto, uma diferença de tratamento entre os requisitos das seções 4 a 8 e os controles do anexo A, em que não se admite exclusão para aqueles, e sim apenas para esses, desde que devidamente justificados.

Um equívoco comum ao se configurar um ISMS é o fato de se voltar mais para os controles sem se atentar para os requisitos das seções 4 a 8 da norma ISO 27001:2005, pois, em alguns casos, não basta ter determinado controle para estar em conformidade com essa norma, fazendo-se necessário que tal controle atenda aos requisitos dessas seções.

Para exemplificar, abaixo, vamos apresentar o item A.5 do anexo A da norma ISO 27001:2005, que trata dos controles e objetivos de controle para a política de segurança da informação.

A.5	POLÍTICA DE SEGURANÇA
A.5.1	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO Objetivo: Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

[41] A lista apresentada no anexo A da norma não é exaustiva, devendo a organização ter a liberdade para adicionar outros controles que julgar necessários.

A.5.1.1	Documento da política de segurança da informação	Controle Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica da política de segurança da informação	Controle A política de segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Quando da verificação dos controles, deve-se evidenciar que a organização possui uma política de segurança da informação documentada (item A.5.1.1) e aprovada pela direção, publicada e comunicada a todos os funcionários e partes relevantes. Isso por si só não significa que a organização esteja alinhada com a norma, porque a política de segurança da informação possui requisitos específicos, que devem atender aos requisitos da seção 4 (item 4.2.1 b), que diz:

> b) Definir uma política do ISMS nos termos das características do negócio, a organização, sua localização, ativos e tecnologia que:
>
> 1) inclua uma estrutura para definir objetivos e estabeleça um direcionamento global e princípios para ações relacionadas com a segurança da informação;
>
> 2) considere requisitos de negócio, legais e/ou regulamentares, e obrigações de segurança contratuais;
>
> 3) esteja alinhada com o contexto estratégico de gestão de riscos da organização, no qual o estabelecimento e manutenção do ISMS irão ocorrer;

4) estabeleça critérios em relação aos quais os riscos serão avaliados; e
5) tenha sido aprovada pela direção.

Esse exemplo mostra a importância de se observarem os requisitos das seções 4 a 8, pois não basta se ter uma política documentada, aprovada pela direção e divulgada, como está estabelecido no anexo A (exemplo acima) para se obter a conformidade. É indispensável que tal política atenda aos requisitos da seção 4.2.1 b para se obter a conformidade, nesse item.

De certa forma, pode-se concluir que a formatação do ISMS deve ser fundamentada nos requisitos das seções 4 a 8, e consolidada com a implementação dos controles listados no anexo A da referida norma.
Abaixo estão reproduzidos os objetivos de controle do anexo A da norma ISO 27001:2005:[42]

A.5 Política de segurança
A.5.1 Política de segurança da informação
Objetivo: Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.

A.6 Organizando a segurança da informação
A.6.1 Organização interna
Objetivo: Gerenciar a segurança da informação na organização.
A.6.2 Partes externas
Objetivo: Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados, ou gerenciados por partes externas.

A.7 Gestão de ativos
A.7.1 Responsabilidade pelos ativos
Objetivo: Alcançar e manter a proteção adequada dos ativos da organização.
A.7.2 Classificação da informação

[42] Cada item de objetivo de controle é subdividido em controles, que não estão aqui relacionados.

Objetivo: Assegurar que a informação receba um nível adequado de proteção.

A.8 Segurança nos recursos humanos

A.8.1 Antes da contratação

Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos.

A.8.2 Durante a contratação

Objetivo: Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.

A.8.3 Encerramento ou mudança da contratação

Objetivo: Assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.

A.9 Segurança física e do ambiente

A.9.1 Áreas seguras

Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

A.9.2 Segurança de equipamentos

Objetivo: Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.

A.10 Gerenciamento das operações e comunicações

A.10.1 Procedimentos e responsabilidades operacionais

Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.

A.10. 2 Gerenciamento de serviços terceirizados

Objetivo: Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em linha com acordos de entrega de serviços terceirizados.

A.10.3 Planejamento e aceitação dos sistemas

Objetivo: Minimizar o risco de falhas nos sistemas.

A.10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do *software* e da informação.
A.10.5 Cópias de segurança
Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.
A.10.6 Gerenciamento da segurança em redes
Objetivo: Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte.
A.10.7 Manuseio de mídias
Objetivo: Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio.
A.10.8 Troca de informações
Objetivo: Manter a segurança na troca de informações e *softwares* internamente à organização e com quaisquer entidades externas.
A.10.9 Serviços de comércio eletrônico
Objetivo: Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.
A.10.10 Monitoramento
Objetivo: Detectar atividades não autorizadas de processamento da informação.

A.11 Controle de acessos
A.11.1 Requisitos de negócio para controle de acesso
Objetivo: Controlar o acesso à informação.
A.11.2 Gerenciamento de acesso do usuário
Objetivo: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.
A.11.3 Responsabilidades dos usuários
Objetivo: Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.
A.11.4 Controle de acesso à rede
Objetivo: Prevenir acesso não autorizado aos serviços de rede.
A.11.5 Controle de acesso ao sistema operacional
Objetivo: Prevenir acesso não autorizado aos sistemas operacionais.
A.11.6 Controle de acesso à aplicação e à informação

Objetivo: Prevenir acesso não autorizado à informação contida nos sistemas de aplicação.

A.11.7 Computação móvel e trabalho remoto

Objetivo: Assegurar a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.

A.12 Aquisição, desenvolvimento e manutenção de sistemas de informação

A.12.1 Requisitos de segurança de sistemas de informação

Objetivo: Garantir que segurança é parte integrante de sistemas de informação.

A.12.2 Processamento correto de aplicações

Objetivo: Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.

A.12.3 Controle criptográfico

Objetivo: Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.

A.12.4 Segurança dos arquivos do sistema

Objetivo: Garantir a segurança de arquivos de sistema.

A.12.5 Segurança em processos de desenvolvimento e de suporte

Objetivo: Manter a segurança de sistemas aplicativos e da informação.

A.12.6 Gestão de vulnerabilidades técnicas

Objetivo: Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.

A.13 Aquisição, desenvolvimento e manutenção de sistemas de informação

A.13.1 Gestão de incidentes de segurança da informação

Objetivo: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação em tempo hábil.

A.13.2 Gestão de incidentes de segurança da informação e melhorias

Objetivo: Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.

A.14 Gestão da continuidade do negócio

A.14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação

Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil, se for o caso.

A.15 Conformidade

A.15.1 Conformidade com requisitos legais

Objetivo: Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.

A.15.2 Conformidade com normas e políticas de segurança da informação e conformidade técnica

Objetivo: Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.

5 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: O PONTO DE PARTIDA

Nos capítulos anteriores deste livro, foram abordados diversos assuntos relacionados com a segurança da informação, começando por se compreender a informação, suas vulnerabilidades e ameaças, passando pelo estudo e gerenciamento de riscos até o sistema específico para a segurança da informação. Tudo isso serve de fundamentação para que se possa transformar a intenção de se proteger a informação em uma política específica voltada para a segurança da informação.

É justamente com esse assunto que concluímos este livro, por onde tudo deve começar: **a política de segurança da informação**.

Para nós, a política é a materialização da intenção do que desejamos fazer, e essa intenção é transformada em princípios, valores, compromissos, requisitos, objetivos e orientações sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações.

Nesse sentido, pode-se definir a política de segurança da informação como: um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades para com a segurança da informação.

A sua forma, escopo e detalhes estão diretamente relacionados com as atividades de negócios e decisão da organização do nível e padrão de segurança que se pretende alcançar.

Existem vários tipos de políticas, entretanto a norma ISO 27002:2005 (item 5.1.1), ao apresentar as diretrizes para uma política de segurança da informação, afirma que esse documento deve conter:

> a) Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação;
> b) Uma declaração de comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégia de negócios;

c) Uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de avaliação e gerenciamento de riscos;
d) Breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:
    1) Conformidade com a legislação e com requisitos regulamentares e contratuais;
    2) Requisitos de conscientização, treinamento e educação em segurança da informação;
    3) Gestão da continuidade do negócio;
    4) Consequências das violações na política de segurança da informação
e) Definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;
f) Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas específicos ou regras de segurança que os usuários devem seguir.

Essa norma orienta ainda que a política deve ser comunicada a toda a organização para os usuários, de forma que seja relevante, acessível e compreensível para o leitor em foco.

Uma questão que merece destaque com relação a uma política de segurança da informação diz respeito aos controles, pois algumas políticas são elaboradas com a descrição de todos os controles, e, às vezes, possuem a reprodução de todos os controles do anexo A da norma ISO 27001:2005, quando se pretende conformidade com essa norma.

Como a política deve ser divulgada por toda a organização, e ela é o ponto de partida para a segurança da informação, assunto até certo ponto áspero, a adoção dessa linha de ação (se detalhar todos esses controles) não parece ser uma decisão que venha facilitar o processo de cultura pela segurança da informação.

A melhor estratégia parece ser a de os controles serem apresentados de uma maneira geral, podendo ser resumidos em poucos itens, pois o

objetivo que se quer alcançar com os funcionários é a implementação de uma nova prática para a realização dos negócios com mais segurança, e isso será alcançado com a mudança de cultura, o que, dependendo da forma como a política seja apresentada, poderá ser mais rápido ou até inatingível.

Outra questão diz respeito à divulgação e ao treinamento. O primeiro passo é fazer com que as pessoas compreendam o que seja a informação e a sua importância no ambiente das atividades de negócios, as ameaças a ela e suas vulnerabilidades e o porquê de protegê-la. A partir dessa percepção, deve-se apresentar a política de segurança da informação e iniciar uma verdadeira campanha pela sua completa realização.

O exemplo dos diretores e gerentes é outro ponto crucial no sucesso de uma política, pois os funcionários estarão atentos às atividades dessas pessoas com relação a essa mudança de cultura, e, se o exemplo não vier deles, a imagem que se passará será a de mais um documento de gaveta, apenas para se ter e não para valer.

Para melhor entendimento do assunto deste capítulo, abaixo está apresentado um exemplo de uma política de segurança da informação de uma organização aqui denominada de MD. Esse exemplo está alinhado com a norma ISO 27002:2005 e atende aos requisitos de conformidade da norma ISO 27001:2005.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA MD

1. Introdução

A evolução da tecnologia mudou a forma dos negócios. Hoje, o centro nervoso da nova estrutura dos negócios corporativos está no sistema de informações.

O nosso sistema de informações é constituído por um conjunto de elementos ou componentes inter-relacionados, que coletam, manipulam e disseminam os dados e a informação para as nossas atividades de negócios. Ele é composto de *hardware*, *software*, bancos de dados, telecomunicações, pessoas e procedimentos, que formam a infraestrutura tecnológica da nossa organização. Hoje, esses sistemas são essenciais e críticos para o sucesso das atividades de negócios da nossa organização.

O ambiente de negócios não é mais delimitado como antes, agora é, também, o ciberespaço. O mundo virtual e a sua capacidade de processamento objetivam melhorar e facilitar as atividades de negócios, porém trazem consigo ameaças à segurança da informação e aos negócios da organização.

Para interromper uma atividade de negócio, não se faz necessário um atentado terrorista ou um evento da natureza de proporção catastrófica. Para que isso aconteça, basta uma simples ação de um funcionário que, agindo intencionalmente ou não, pratica uma ação que compromete as qualidades da informação e o sucesso dos negócios corporativos, e que, às vezes por sorte, não provocam danos como: fraudes financeiras, ataques de vírus, invasão e indisponibilidade de sistemas, etc.

É com foco nesse cenário que a nossa organização decidiu adotar uma filosofia moderna de segurança da informação, com a finalidade de constituir um sistema de segurança da informação alinhado com o padrão internacional das normas ISO, para que nossos funcionários, clientes, fornecedores, colaboradores e acionistas possam desempenhar seus papéis certos de que o fazem em um ambiente seguro.

Para isso ser possível, apresentamos neste documento um conjunto de intenções, diretrizes e procedimentos gerais da nossa empresa, que denominamos de **política de segurança da informação.**

2. Objetivo

A nossa política de segurança da informação tem como objetivo geral prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentos.

Possui também os seguintes objetivos específicos:

1- Proporcionar a segurança da informação na organização;
2- Fomentar a cultura pela segurança da informação nos funcionários, acionistas, clientes, fornecedores e colaboradores;
3- Estabelecer ações necessárias à implementação e à manutenção da segurança da informação baseadas nos principais riscos aos negócios corporativos;
4- Obter a certificação da norma ISO 27001:2005.

Para que esses objetivos sejam alcançados, faz-se necessária a implementação de um sistema de gestão de segurança da informação (ISMS), alinhado com as diretrizes da norma ISO 27002:2005 e em conformidade com os requisitos da norma ISO 27001:2005, que é o padrão de segurança da informação adotado por esta organização.

3. Compromisso da direção

Conscientes da importância das informações para os negócios corporativos e a continuidade das atividades, e considerando os objetivos acima estabelecidos, nós, diretores abaixo assinados, nos comprometemos a cumprir essa política de segurança da informação, bem como dispender os esforços necessários à sua implementação e quaisquer ações voltadas à garantia da conformidade com o padrão de segurança da informação estabelecido pela organização.

4. Conformidade com a legislação

A presente política está em conformidade com a legislação vigente, e de acordo com as garantias e direitos individuais e coletivos das pessoas, a inviolabilidade da sua intimidade e o sigilo da correspondência e das comunicações, no termos da Constituição Federativa da República do Brasil em vigor.

]

5. Segurança da informação

No seu contexto maior, a segurança da informação compreende as ações para a proteção da informação e de seus ativos contra os vários tipos de ameaças, com a finalidade de garantir a continuidade das atividades da nossa organização.

O conceito adotado para a segurança da informação é o estabelecido na norma ISO/IEC 27002:2005, que é a *"Preservação da confidencialidade, da integridade e da disponibilidade da informação"*. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Para isso, a nossa organização adota os seguintes princípios para a segurança da informação:

Autenticidade: é a garantia de que a informação é legítima, oriunda da fonte que lhe é atribuída e elaborada por quem tem autoridade para tal.
Confiabilidade: é a garantia de que a informação é confiável, oriunda de uma fonte idônea e expressa uma mensagem verdadeira.
Confidencialidade: é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso (ISO/IEC 27002:2005).
Conformidade: é a garantia de que as atividades são desempenhadas de acordo com as normas, padrões e controles estabelecidos.
Disponibilidade: é a garantia de que os usuários autorizados vão obter acesso à informação e aos ativos correspondentes sempre que necessário (ISO/IEC 27002:2005).
Integridade: é a garantia da exatidão e completeza da informação e dos métodos de processamento (ISO/IEC 27002:2005).
Investigação: é a garantia de que toda e qualquer investigação será motivada, realizada por pessoal competente, com procedimentos definidos, e não atentará contra os direitos e garantias individuais.
Legalidade: é a garantia de que todas as ações voltadas para a segurança da informação estão de acordo com as leis em vigor.
Não repúdio: é a garantida de que a informação chegará ao destino certo e não será repudiada.
Privacidade: é a garantia da preservação de dados e informações pessoais da ação de bisbilhotar.
Responsabilidade: é a coparticipação de responsabilidade por todos que produzem, manuseiam, transportam e descartam a informação, seus sistemas e redes de trabalho (*network*).

6. Estrutura de controles

Um comitê específico para a segurança da informação cuidará do planejamento da infraestrutura e das ações voltadas para a segurança da informação.

A estrutura de controles adotada para se alcançarem os objetivos da segurança da informação é baseada numa criteriosa análise dos principais riscos que afetam a informação, seus ativos e os principais negócios da organização.

Após serem identificados, esses riscos devem ser avaliados, selecionados pela sua criticidade e submetidos às medidas de tratamento aprovadas pela diretoria.

A metodologia de avaliação dos riscos deve ser adequada aos requisitos de negócios da organização e devidamente justificada, podendo ser utilizada uma ferramenta de avaliação de riscos.

Contudo, tanto a metodologia quanto a ferramenta devem ser as mesmas para o processo de avaliação de todos os riscos, não podendo ser utilizado um padrão diferente para a metodologia, nem tampouco critérios de aceitabilidade diferentes para a análise em questão. O padrão escolhido deve ser o mesmo até o final da avaliação, independentemente da criticidade do risco em análise.

Os controles estabelecidos com base na análise efetuada têm uma finalidade específica descrita no seu objetivo de controle, que é a justificativa para o qual cada controle deve ser criado. Cada controle deverá ter domínio específico e estar devidamente descriminado no documento denominado **declaração de aplicabilidade**.

Esse documento deve ser referenciado nos controles estabelecidos no anexo A da norma ISO 27001:2005, com a indicação dos controles já implementados, bem como a justificativa daqueles que forem devidamente excluídos.

A avaliação de riscos deverá ser revisada em períodos de tempo determinados, ou toda vez que seja necessária, ou ocorra fato que mereça atenção.

Os controles deverão ser periodicamente auditados para o exame da sua eficácia e avaliação quanto ao objetivo para o qual foram estabelecidos. Essa avaliação poderá ser feita com base nos controles aplicáveis ou em níveis de maturidade previamente estabelecidos.

As auditorias poderão ser realizadas por pessoal interno, por auditor independente, ou por organização de auditoria, desde que sejam devidamente qualificados para tal atividade.

As recomendações da auditoria deverão ser implementadas dentro do prazo estabelecido e submetidas a novo exame, bem como as ações corretivas e preventivas.

7. Treinamento

Os treinamentos em segurança da informação devem alcançar todos os funcionários e ser graduados mediante a criticidade das atividades para a organização, e devem incluir palestras, *workshops*, seminários, cursos de extensão e especialização.

Deve ser o objetivo principal dos treinamentos a conscientização e o fomento à cultura da segurança da informação, bem como o exercício das atividades funcionais dentro dos requisitos de segurança estabelecidos pela organização.

Anualmente, deverá ser realizado um seminário sobre segurança da informação, no qual constem, dentre os painéis, as experiências vivenciadas na organização.

Uma série de orientações gerais e específicas sobre segurança da informação deverá estar disponível para consulta *on-line* pelos funcionários. Essas orientações podem estar em arquivos texto, em vídeos, ou em *links* devidamente identificados.

Os clientes, fornecedores, colaboradores e acionistas deverão receber orientações gerais sobre os procedimentos a serem adotados com relação à segurança da informação na nossa organização.

8. Gestão da continuidade

A gestão da continuidade das atividades da organização deve ser baseada em processos e atividades que incluam prevenção, detecção, resposta e recuperação de eventos indesejáveis e danosos à segurança da informação e à continuidade das atividades de negócios, e deve ter dotação específica no orçamento geral da organização.

Uma avaliação de impacto nos negócios deve ser realizada para identificar os impactos nas atividades críticas de negócios, cuja análise deve considerar o tempo de aceitabilidade da interrupção, a perda financeira, o tempo para a recuperação e a relação custo-benefício das medidas de continuidade a serem adotadas.

As medidas de continuidade devem incluir as ações de respostas imediatas ao evento, as ações para garantir a *performance* mínima para a continuidade das atividades, assim como as ações de recuperação e

restauração do *status quo* anterior à materialização do evento, devendo constar do documento denominado: **plano de continuidade de negócios.**

9. Atribuições e responsabilidades

As atribuições e responsabilidades descritas neste documento referem-se às atividades genéricas com relação à segurança da informação, não se constituindo em ponto limitador ao estabelecimento de regras específicas para as atividades cotidianas de negócios da organização com relação à segurança da informação.

Compete à diretoria da organização:

- ✓ Dar o bom exemplo no cumprimento das medidas de controle estabelecidas para a segurança da informação;
- ✓ Aprovar as políticas, normas e procedimentos de segurança da informação;
- ✓ Apoiar ativamente as medidas de segurança dentro da organização;
- ✓ Patrocinar as iniciativas, campanhas, seminários e treinamentos voltados para a segurança da informação;
- ✓ Disponibilizar recursos quando necessário, e
- ✓ Promover a avaliação periódica dos controles estabelecidos.
- ✓

Compete ao Comitê Gestor de Segurança da Informação (CGSI):

O Comitê Gestor de Segurança da Informação (CGSI) é um colegiado criado com a finalidade de **coordenar a segurança da informação**, e será presidido pelo diretor de tecnologia da informação.

O Comitê surge da necessidade de se padronizarem procedimentos em situações normais, e de equacionarem determinadas situações críticas (crises ou desastres), passíveis de consequências mais sérias, que exigem um tratamento específico focado em posturas administrativas e operacionais voltadas para eliminar improvisos e gastos desnecessários, viabilizando a melhor alternativa para superar tais situações, a fim de se garantir o retorno à normalidade das atividades da organização.

São membros permanentes do Comitê:

1- O diretor de TI que presidirá o Comitê;

2- O diretor financeiro;

3- O diretor de planejamento ou seu representante;
4- O diretor de RH ou seu representante;
5- O responsável pela segurança corporativa, e
6- Dois funcionários da diretoria de TI.

Como membro convidado, poderá participar qualquer funcionário da organização, bem como especialistas em segurança da informação ou área de interesse.

São atribuições do CGSI:

1- Ser responsável pelo desenvolvimento, análise crítica e avaliação da política de segurança da informação (SI);
2- Desenvolver atividades para que a SI seja exercida em conformidade com a política de segurança da informação;
3- Orientar a condução das não conformidades, bem como a sua correção;
4- Aprovar as metodologias e processos para a SI;
5- Identificar as principais ameaças, as exposições da informação e dos recursos de processamento a essas ameaças;
6- Avaliar a adequação dos controles de SI, bem como a sua implementação;
7- Promover a educação, o treinamento e a conscientização pela SI de toda a organização;
8- Avaliar as informações recebidas do monitoramento e da análise crítica dos incidentes de SI, bem como recomendar as ações para as respostas aos incidentes identificados;
9- Gerenciar as crises e desastres relacionados com SI, no âmbito da organização;
10- Aplicar, supervisionar e avaliar as medidas necessárias para a resolução dessas situações, com autonomia e responsabilidade nas deliberações durante o período de duração desses cenários;
11- Avaliar as medidas emergenciais empregadas nos eventos e incidentes de SI;
12- Avaliar a aplicabilidade ou não dos controles estabelecidos na Declaração de Aplicabilidade (SoA);
13- Manter contato com organizações externas para ajuda mútua e troca de experiências em casos relacionados com SI;

14- Avaliar e aprovar as sanções propostas pelo descumprimento das normas e procedimentos de SI.

Cada gestor é responsável pela segurança das informações produzidas, manuseadas, arquivadas e descartadas pelo seu setor, bem como pelas boas práticas de utilização dos equipamentos e da rede corporativa.

Todo e qualquer funcionário tem o dever de ter conhecimento e de zelar por essa política de segurança da informação, e é responsável pelo fiel cumprimento das normas e procedimentos de segurança estabelecidos, bem como comunicar qualquer evento ou incidente de SI de que tiver conhecimento ao setor de tecnologia da informação.

Os **prestadores de serviço, colaboradores, clientes, fornecedores e representantes do poder público** devem zelar pelo cumprimento das normas e procedimentos de segurança estabelecidos. Devem, também, comunicar qualquer evento ou incidente de segurança de que tiverem conhecimento ao setor de tecnologia da informação.

10. Políticas gerais de segurança da informação

As políticas abaixo apresentadas constituem os requisitos fundamentais para a segurança da informação, e foram estabelecidas dentro do contexto de negócios da organização.

1. Os sistemas de informações são indispensáveis às atividades de negócios da organização, e compõem todo um arcabouço de políticas, procedimentos, recursos humanos, tecnologia e infraestrutura, devendo ser protegidos contra quaisquer ameaças ao seu funcionamento.
2. Os ativos de informação e o ambiente informatizado devem estar em conformidade com esta política, normas e procedimentos relativos à segurança da informação, e devem ser protegidos contra ações intencionais ou acidentais que impliquem perda, destruição, inserção, cópia, extração, alteração, uso e exposição indevidos, em conformidade com os princípios de segurança da informação adotados pela organização.
3. As medidas de proteção devem ser adotadas de forma proporcional aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente de negócios, o valor e a criticidade da informação, ou outros critérios estabelecidos para a avaliação de riscos.

4. As informações devem ser classificadas em função de sua importância e confidencialidade, e devem ser mantidas com um nível de proteção adequado ao meio em que sejam produzidas, manuseadas, transportadas, arquivadas e descartadas.
5. O acesso aos ativos de informação e ao ambiente informatizado deve ser sempre motivado por necessidade de serviço, devendo ser controlado e restrito às pessoas autorizadas.
6. O acesso à informação não gera direito real sobre a mesma nem sobre os frutos de sua utilização, e essas informações devem ser tratadas como confidenciais e usadas especialmente para atividades de trabalho, em que a responsabilidade por assegurar a proteção, o uso e o descarte das informações críticas ou sigilosas do setor é do gestor do departamento.
7. As permissões de acesso são de uso exclusivo e intransferível, não podendo a pessoa autorizada deixar qualquer ativo de informação em condições de ser utilizado com suas permissões de acesso por terceiros. Essas permissões de acesso devem ser graduadas de acordo com as atribuições dos funcionários, e os níveis de acesso dos funcionários devem ser determinados pelos gerentes, supervisores e chefes de departamento.
8. O acesso aos sistemas de informações deve ser controlado e realizado mediante senha de acesso. Essa senha deve ser pessoal e de conhecimento restrito do usuário, que é o responsável pela manutenção de seu segredo e pelas consequências de sua divulgação.
9. A organização deve estabelecer procedimentos para a criação de senhas de acesso, e que as mesmas não sejam facilmente descobertas e/ou quebradas por agentes externos.
10. Todo e qualquer acesso aos sistemas deve ser autorizado, e sua solicitação deve ser feita pelo gestor imediato, a quem compete, também, liberar o acesso após sua concessão. Os diretores farão a sua própria solicitação e terão os seus acessos liberados pelo gerente de TI.
11. Os acessos de pessoal externo aos sistemas de informação, na organização e via *internet*, devem ser autorizados pela gerência de TI e monitorados pelo setor de TI. O *site* da organização na *internet* deve ter mecanismos para não se permitir o acesso indevido e não autorizado aos sistemas corporativos.

12. Os funcionários devem ser permanentemente treinados e capacitados para exercer atividades inerentes à área de segurança da informação, bem assim às formas de proteção dos ativos de informação sob sua responsabilidade, de acordo com programa de educação estabelecido pela organização.

13. Os usuários devem ser instruídos para não abrir arquivos recebidos por meio de mensagens de remetentes desconhecidos, ou quando não solicitados e confirmados, como também a não instalar *software* ou jogos eletrônicos nos equipamentos da organização, além de não poderem permitir que um visitante conecte qualquer equipamento a um ponto de acesso da rede de computadores.

14. As saídas com mídias magnéticas gravadas com informações da organização e com documentos impressos por funcionários só podem ser feitas quando autorizadas e para a realização de serviços externos. Essa autorização deve ser dada pelo chefe do departamento ou gerente imediato.

15. Toda e qualquer pesquisa sobre o ambiente computacional, sobre as atividades da organização e sobre funcionários deve ser respondida pelos setores específicos da atividade em questão. Tais pesquisas ou solicitações não devem ser respondidas por telefone, a fim de se minimizar o impacto dos ataques por meio de técnica de "Engenharia Social".

16. O ambiente informatizado deve possuir:

I - modelo de gestão alinhado com os requisitos da norma ISO 27001:2005;

II - plano de contingência que assegure a operação e a recuperação de ativos de informação em situações de emergência, de acordo com as necessidades e prazos específicos;

III - recursos de autenticação para garantir a identificação individual e inequívoca do usuário, quando do acesso aos ativos de informação;

IV - recursos de criptografia;

V - mecanismos de proteção da rede, inclusive em suas interfaces com outras redes e com a *Internet*;

VI – monitoração, em tempo real, com vistas a prover mecanismos para a prevenção, a detecção, a identificação e o combate à invasão (intrusão);

VII - mecanismos para a prevenção, a detecção e a eliminação de *vírus* de computador e de outros programas maliciosos;

VIII - sistemática para a geração de cópia de segurança (*backup*) e de recuperação da informação (*restore*) devidamente documentada, que inclua a periodicidade de cópias, a forma e o local de armazenamento, a autorização de uso, o prazo de retenção e o plano de simulação e testes;

IX - medidas para a verificação dos dados quanto a sua precisão e consistência;

X - registro de informações (log) com os prazos de retenção e as formas de acesso definidas, com vistas a permitir a recuperação do sistema em caso de falha;

XI - registro de informações (trilha de auditoria) com os prazos de retenção e as formas de acesso definidas, com vistas a permitir a auditoria, a identificação de situações de violação e a contabilização individual do uso dos sistemas;

XII - parâmetros de normalidade de utilização definidos, e

XIII - controle de acesso físico às instalações e equipamentos.

17. Os ambientes de produção, treinamento, prospecção, testes, homologação e desenvolvimento dos sistemas informatizados, localizados nas nossas dependências ou em seus prestadores de serviços, devem ser distintos e de exclusividade da organização.

18. As alterações nos sistemas de informações só poderão ser realizadas pelos analistas de TI e mediante solicitação de um gestor. Essas alterações apenas podem entrar em produção quando validadas pelo responsável da demanda e autorizadas pelo gerente de TI.

19. O desenvolvimento de *software* em todas as fases do processo, a prospecção de produtos e serviços e os procedimentos de homologação deverão contar com a participação de funcionários em exercício na área de segurança da informação.

20. Na organização só podem ser utilizados *softwares* licenciados e homologados pelo setor de TI, exceto quanto aos ambientes de prospecção, testes e homologação.

21. Os *softwares* instalados nos equipamentos dos servidores, nos equipamentos de rede e comunicação e nas estações de trabalho devem ser

permanentemente atualizados, visando incrementar aspectos de segurança e corrigir falhas.

22. Os ativos de informação devem ser inventariados periodicamente por funcionários em exercício na área de tecnologia da informação, em relação aos aspectos atinentes a *hardware*, *software* e configurações.

23. A eliminação de informação protegida por sigilo ou de uso exclusivo de setores críticos de negócios da organização e de *softwares* instalados, constantes em dispositivos de armazenamento, deve ser procedida com a utilização de ferramentas adequadas à eliminação segura dos dados, quando:

I - destinados a outro funcionário ou setor de atividade;

II - houver alteração das atividades desempenhadas pelo funcionário e o conteúdo armazenado for indispensável às novas atividades;

III - destinados a pessoas ou organizações não autorizadas, e

IV - o dispositivo de armazenamento estiver danificado. Nesse caso, o dispositivo de armazenamento deverá ser destruído se as informações nele contidas não puderem ser eliminadas.

24. Medidas adicionais de proteção devem ser adotadas, visando garantir o mesmo nível de segurança das instalações internas no caso de:

I - computação móvel;

II - acesso remoto ao ambiente informatizado;

III - operação de redes instaladas em recintos diferentes da organização;

IV - equipamentos destinados ao acesso público, e

V - comunicação sem fio.

25. O tráfego de informações em redes locais e de longa distância deve ser protegido contra danos, perdas, indisponibilidades, uso ou exposição indevidos, de acordo com seu valor, criticidade e confidencialidade. O tráfego de dados deve ser efetuado por meio de canais privativos, sejam eles físicos ou virtuais, que possam prover a criptografia e a autenticação. As redes devem possuir rotas alternativas e contar com mecanismos de redundância.

26. É vedada a alteração dos mecanismos e configurações definidos pelo setor de TI, incluindo:

I - infraestrutura elétrica;

II - infraestrutura lógica;

III - equipamentos de rede e de conectividade;

IV - equipamentos servidores;

V - estações de trabalho fixas;
VI - estações de trabalho móveis;
VII - sistemas operacionais;
VIII - *softwares* em geral; e
IX - dispositivos de comunicação sem fio.

11. Consequências das violações na política de segurança da informação

Os diretores, gerentes, funcionários, prestadores de serviço, colaboradores, clientes, fornecedores e representantes do poder público respondem solidariamente de modo proporcional ao dano causado pela inobservância das políticas, normas e procedimentos estabelecidos e em vigor na organização, relacionados com a segurança da informação.

Procedimentos específicos devem ser criados para a apuração de condutas internas relacionadas com a não observância dos controles e as regras de segurança da informação estabelecidas.

Uma comissão ou um funcionário poderá ser designado para essas apurações, devendo no final apresentar um relatório descritivo para a avaliação e aplicação da penalidade pelo comitê gestor de SI.

A sanção por descumprimento das normas e procedimentos de SI só poderá ser aplicada após o devido procedimento administrativo que assegure os princípios constitucionais da ampla defesa e do contraditório. Deve-se levar em consideração na aplicação das penalidades por esses descumprimentos a vida funcional do profissional, o tempo de serviço na organização e no setor de atividade, assim como o dano por ele causado.

É requisito fundamental para a aplicação de qualquer sanção relacionada com o descumprimento das normas e procedimentos de SI o prévio conhecimento dessas normas e procedimentos, bem como documentação no qual conste o registro do funcionário em treinamento específico de SI e o registro de termo de compromisso e/ou acordos de confidencialidade.

Os termos e os acordos poderão ser em documentos impressos ou em meio eletrônico, devidamente assinados ou registrados, respectivamente.

BIBLIOGRAFIA

Associação Brasileira de Normas Técnicas (ABNT)**. NBR ISO/IEC 27002:2005** – **Tecnologia da informação – Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005.

Associação Brasileira de Normas Técnicas (ABNT)**. NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança – Sistema de gestão de segurança da informação - requisitos**. Rio de Janeiro: ABNT, 2006.

AS/NZS 4360:2004 Risk Management. Third edition. Sydney/Wellington: Standards Australia/Standards New Zealand, 2004.

ACADEMIA LATINO AMERICANA DE SEGURANÇA DA INFORMAÇÃO. Disponível em: <http://www.technetbrasil.com.br/academia.

Australia's National Computer Emergency Response Team (AusCERT), NSW Police and Deloitte Touche Tohmatsu, **2002 Australian Computer Crime and Security Survey**. AusCERT, 2002.

Australia's National Computer Emergency Response Team (AusCERT), Australian Federal Police, Queensland Police, South Australia Police and Western Australia Police. **2003 Australian Computer Crime and Security Survey**. AusCERT, 2003.

Australia's National Computer Emergency Response Team (AusCERT), Australian High Tech Crime Centre, the Australian Federal Police, New South Wales Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police and Western Australia Police. **2004 Australian Computer Crime and Security Survey**. AusCERT, 2004.

Australia's National Computer Emergency Response Team (AusCERT), Australian High Tech Crime Centre, the Australian Federal Police, New South Wales Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police and Western Australia Police. **2005 Australian Computer Crime and Security Survey**. AusCERT, 2005.

Australia's National Computer Emergency Response Team (AusCERT), Australian High Tech Crime Centre, the Australian Federal Police, New South Wales Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police and Western Australia Police. **2006 Australian Computer Crime and Security Survey**. AusCERT, 2006.

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

BRASIL. **Decreto nº 4.553, de 27 de novembro de 2002**. Diário Oficial da União, poder Executivo, Brasília, 30/12/2002.

BRASILIANO, Antonio Celso Ribeiro. **Planejamento da segurança empresarial – metodologia e implantação**. São Paulo: Brasiliano & Associados: Sicurezza: Cia. Das Artes, 1999.

BRASILIANO, Antonio Celso Ribeiro. **Manual de planejamento: gestão de riscos corporativos**. São Paulo:Sicurezza, 2003.

BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management. British Standards Institution (BSI): 2006.

BUSINESS CONTINUITY PLANNING GUIDE (BCPG). First edition. Property Advisers to the Civil Estate (PACE): Central Advice Unit, may, 1998.

CARDOSO JÚNIOR, Walter Felix. **Inteligência empresarial estratégica**. Tubarão:Ed. Unisul, 2005.

CASADA, Myron; Thomas Nolan; David Trinker; and David Walker. **Guide for Port Security**. Houston: ABS Consulting, Octuber, 2003.

Computer Security Institute (CSI), and Federal Bureau of Investigation (FBI). **2003 CSI/FBI Computer Crime and Security Survey**. CSI/FBI, 2003.

Computer Security Institute (CSI), and Federal Bureau of Investigation (FBI). **2004 CSI/FBI Computer Crime and Security Survey**. CSI/FBI, 2004.

Computer Security Institute (CSI), and Federal Bureau of Investigation (FBI). **2005 CSI/FBI Computer Crime and Security Survey**. CSI/FBI, 2005.

Computer Security Institute (CSI), and Federal Bureau of Investigation (FBI). **2006 CSI/FBI Computer Crime and Security Survey**. CSI/FBI, 2006.

Computer Security Institute (CSI), and Federal Bureau of Investigation (FBI). **2007 CSI/FBI Computer Crime and Security Survey**. CSI/FBI, 2007.

DANTAS, Marcus Leal. **Segurança preventiva: conduta inteligente do cidadão**. Recife: Nossa livraria, 2003.

Deloitte Touche Tohmatsu. **2005 Global Security Survey**. London: Deloitte, 2005.

Deloitte Touche Tohmatsu. **2006 Global Security Survey**. London: Deloitte, 2006.

GENERAL ACCOUNTING OFFICE (GAO). **Information Security Risk Assessment: pratices of leading organization**. United States: Washington: GAO, 1999.

HB 231:2004 Information Security Risk Management Guidelines. Sydney/Wellington: Standards Australia/Standards New Zealand, 2004.

HB 436:2004 Risk Management Guidelines. Sydney/Wellington: Standards Australia/Standards New Zealand, 2005.

HB 292:2006 A Practitioners Guide to Business Continuity Management. Sydney: Standards Australia, 2006.

HOUAISS DICIONÁRIO DA LINGUA PORTUGUESA. Disponível em: <http://www.houaiss.uol.com.br>. Acesso em 30 out 2005.

INTERNATIONAL MARITIME ORGANIZATION (IMO). **International Ship and Port Facility Security Code (ISPS Code)**. Eletronic Edition. London: International Maritime Organization, 2003.

ISO/IEC 13335-1:2004 – Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.

ISO/IEC Guide 73:2002 – Risk Management – Vocabulary – Guideliness for use in standards. First edition. Switzerland: International Organization for Standardization, 2002.

IT GOVERNANCE INSTITUTE (ITGI). **COBIT 4.1**. Illinois, USA: IT Governance Institute, 2007.

J. Alex Haldermany, Seth D. Schoenz, Nadia Heningery, William Clarksony, William Paulx, Joseph A. Calandrinoy, Ariel J. Feldmany, Jacob Appelbaum. **Lest We Remember: Cold Boot Attacks on Encryption Keys**. New Jersey, Princeton University: Electronic Frontier Foundation, February, 2008. disponível em:<http://citp.princeton.edu.nyud.net/pub/coldboot.pdf>

KUHN, Markus G. **Optical time-domain eavesdropping risks of CRT Displays**. IEEE Symposium on Security and Privacy, Berkeley, California, USA May 12–15, 2002. Disponível em:<http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf>.

LOUGHRY, Joe and UMPHRESS, David A. **Information Leakage from Optical Emanations**. ACM Transactions on Information and System Security (TISSEC), 5(3):262--289, 2002. Disponível em:<http://www.applied-math.org/acm_optical_tempest.pdf>.

MATSUMOTO, Tsutomo, H. Matsumoto, K. Yamada, S. Hoshino. **Impact of artificial "Gummy" fingers on fingerprint systems.** Proceedings of SPIED Vol. #4677, Optical security and counterfeit deterrence techniques IV. Yokohama National University, 14may2002. Disponível em:< http://cryptome.org/gummy.htm>.

MICROSOFT. **Guia de Gerenciamento de riscos de Segurança**. Disponível em: <http://www.microsoft.com/brasil/security/guidance/riscos/default.mspx>. Acesso em 20 abr 2005.

MINTZBERG, H; AHLSTRAND, B; LAMPEL, J. **Safári de estratégia: um roteiro pela selva do planejamento estratégico**. Porto Alegre: Bookman, 2000.

MÓDULO. **Curso Segurança da informação 1 st step**. Rio de Janeiro: Módulo Security Solutions S.A., 2004.

MÓDULO. **8ª Pesquisa Nacional de Segurança da Informação**. Rio de Janeiro: Módulo Security Solutions S.A., 2002.

MÓDULO. **9ª Pesquisa Nacional de Segurança da Informação**. Rio de Janeiro: Módulo Security Solutions S.A., 2003.

OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. Paris: OECD, 2002. www.oecd.org

Operational Critical Threat, Asset, and Vulnerability Evaluation[SM] (**OCTAVE**[SM]). Pittsburgh: Software Engineering Institute: Carnegie Mellon University, 2001. Disponível em: <http:www.cert.org/octave/>.

RALPH, M. Stair e George W. Reynolds. **Princípios de sistemas de informação: uma abordagem gerencial**. 4ª ed. Rio de Janeiro: LTC, 2002.

SÊMOLA, Marcos. **Gestão da segurança da informação: visão executiva da segurança da informação**. Rio de Janeiro:Campus, 2003.

TOIGO, Jon William. **Disaster recovery planning: preparing for the unthinkable**. 3rd ed. New jersey: Prentice Hall, PTR, 2003.

UNITED STATES COAST GUARD. **Navigation and Vessel Inspection Circular 11/2002 - NVIC 11-02**: Recommended Security Guidelines for Facilities. Washington: United States Coast Guard, 2003.

LivroRápido

Serviço de impressão de obras
raras e contemporâneas.

Visite-nos e comprove nossas vantagens

www.livrorapido.com

Rua Dr. João Tavares de Moura, 57/99 - Peixinhos
Olinda/PE - CEP: 53230-290
Fone: (81) 2121.5300 - Fax: (81) 2121.5333
e-mail: livrorapido@webelogica.com

Estar 100% seguro é uma meta a ser perseguida. Um desafio. Se tratar da segurança pessoal já é difícil, imagine-se tratar da segurança da informação, em que a evolução tecnológica é cada dia mais veloz e não alcança toda uma sociedade em todos os seus níveis. Nesse contexto, objetivando proporcionar uma visão abrangente e uma abordagem proativa para a proteção da informação dentro da complexa modernização da sociedade, é que escrevemos este livro.

Marcus Dantas

ISBN 978-85-406-0047-8