Entendendo e implementando a Norma ABNT NBR ISO/IEC 17799:2005

Academia Latino-Americana de Segurança da Informação

Aspectos teóricos e práticos para implantação da Norma

ABNT NBR ISO/IEC 17799:2005

Módulo 1

Entendendo e implementando a Norma ABNT NBR ISO/IEC 17799:2005

Apostila desenvolvida pelo Instituto Online em parceria com a Microsoft Informática

http://www.instonline.com.br/

Revisão 1.1 – Abril de 2006

COORDENADORES TÉCNICOS

Arthur Roberto dos Santos Júnior
Fernando Sérgio Santos Fonseca
Paulo Eustáquio Soares Coelho

COMO USAR ESSE MATERIAL

Este é um material de apoio para o curso “Entendendo e implementando a ABNT NBR ISO/IEC 17799:2005” ministrado pela Academia de Segurança Microsoft. Durante o curso serão apresentados vários Webcasts com o conteúdo deste material acompanhado de slides e voz para ilustrar os conceitos e práticas. A cópia desses slides está em destaque na apostila, seguida de textos com informações que serão abordadas pelo instrutor nos respectivos Webcasts.

LABORATÓRIO : TÍTULO AQUI

Os laboratórios de cada módulo do curso são identificados dessa forma e seu roteiro está especificado sob o título.

VÍDEO

Indica que será apresentado um filme para ilustrar as práticas ou conceitos.

ÍNDICE

APRESENTAÇÃO

Os desafios para a implantação de um ambiente de segurança em qualquer empresa, independente do tamanho, são enormes. O maior problema é implementar as políticas e normas de segurança em um sistema real, que possui aplicações em funcionamento, hardware em produção, softwares proprietários e de terceiros e, acima de tudo, pessoas. É literalmente como trocar o pneu com o carro andando.

Como a maior parte das informações vitais para o sucesso de uma organização reside em computadores, perdas de dados podem ser catastróficas. Os riscos de um negócio com sistema de segurança da informação inadequado são incalculáveis. Segurança da informação é manter a confidencialidade, integridade e disponibilidade da informação. Ela abrange muito mais do que a segurança da informação de TI. Ela cobre a segurança de toda e qualquer informação da empresa, esteja ela em meios eletrônicos, papel ou até mesmo na mente dos funcionários.

Motivados pela busca de soluções para esses desafios, diversos profissionais de várias áreas e organizações, vêem se esforçando para criar normas que sistematizem o trabalho de criar ambientes seguros de TI. Um desses resultados foi consolidado com a norma ABNT NBR ISO/IEC 17799:2005. Utilizando-se essa norma, que é um guia de melhores práticas, simplifica-se o trabalho de adoção e implementação de políticas e padrões definidos, bem como da posterior verificação da conformidade dos resultados alcançados.

O objetivo deste curso é entender as características de alguns padrões de segurança e, em especial, fazer um estudo dos códigos de prática para gestão da segurança da informação contidos na norma ABNT NBR ISO/IEC 17799:2005, proporcionando um entendimento de como implementar, manter e melhorar a gestão da segurança da informação nas empresas.

Ao final deste curso você estará apto a:

- ❒ Entender os padrões empregados para a gestão da segurança da informação;
- ❒ Entender a evolução destes padrões;
- ❒ Descrever os controles contidos na norma ABNT NBR ISO/IEC 17799:2005;
- ❒ Conceituar cada controle da norma;
- ❒ Através de um estudo de caso, implementar a norma em uma empresa.

Capítulo

1

1 - INTRODUÇÃO À ABNT NBR/ISO/IEC 17799:2005

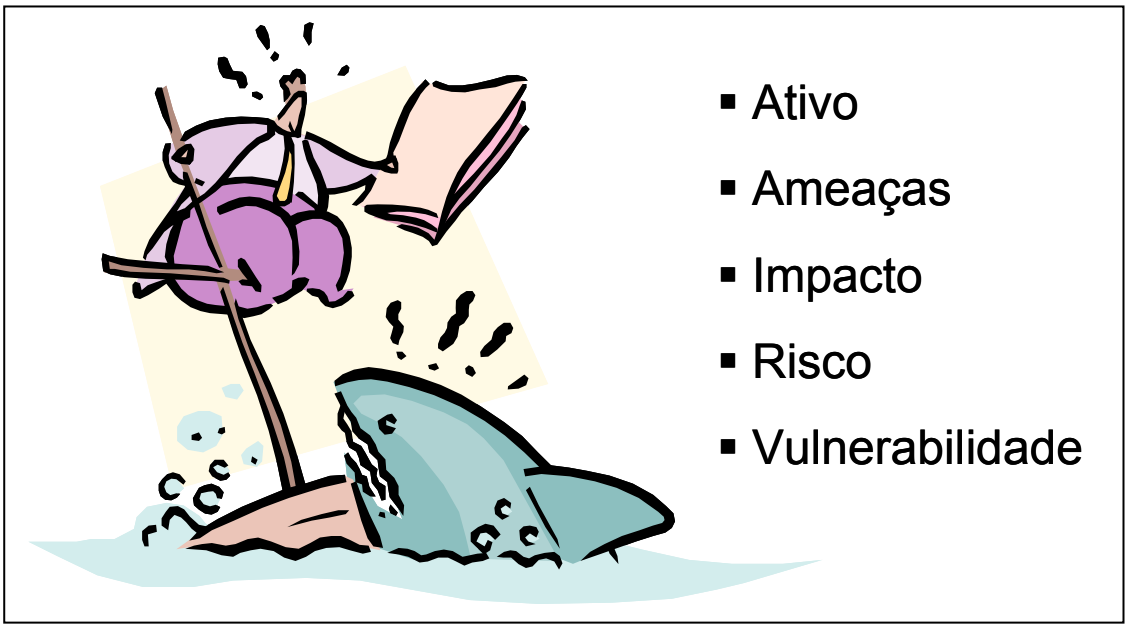
NESTE CAPÍTULO INICIAREMOS O ESTUDO DA NORMA ABNT NBR ISO/IEC 17799:2005. VEREMOS OS CONCEITOS BÁSICOS ABORDADOS PELA NORMA E UMA FORMA PRÁTICA DE INICIAR A IMPLANTAÇÃO DE UM PROCESSO DE PLANEJAMENTO DE GESTÃO E MONITORAMENTO DE SEGURANÇA DE TI.

OBJETIVOS

Neste capítulo veremos os conceitos básicos de segurança da informação, sua definição e passos gerais para sua implantação.

Ao final deste capítulo você estará apto a:

- ❒ Conceituar a segurança da informação;
- ❒ Entender quais as fontes de requisitos de segurança da informação;
- ❒ Entender em linhas gerais quais os passos a serem trilhados para a obtenção de uma ambiente seguro para a informação.



Toda e qualquer informação, que seja um elemento essencial para os negócios de uma organização, deve ser preservada pelo período necessário, de acordo com sua importância. A informação é um bem como qualquer outro e por isso deve ser tratada como um “ativo”.

A interconexão das empresas através de links cabeados e/ou sem fio (wireless), internos e/ou externos, pessoas e ações da natureza, pode expor vulnerabilidades que colocam em risco as informações. Assim, faz-se necessário a implantação de processos de segurança que protejam a informação contra essas ameaças.

A fim de proporcionar o bom entendimento das abordagens que serão feitas nesse curso, é importante conceituarmos alguns termos. Outros não tratados diretamente nesta sessão são descritos ao longo do curso.

- *Ameaça (threat)*: causa potencial de um incidente indesejado, que caso se concretize pode resultar em dano.

- *Ativo (asset)*: é qualquer coisa que tenha valor para um indivíduo ou uma organização, tais como, hardware de computadores, equipamentos de rede, edificações, software, habilidade de produzir um produto ou fornecer um serviço, pessoas, imagem da organização, etc...

- *Incidente de segurança* (security incident)*:* é qualquer evento em curso ou ocorrido que contrarie a política de segurança, comprometa a operação do negócio ou cause dano aos ativos da organização.

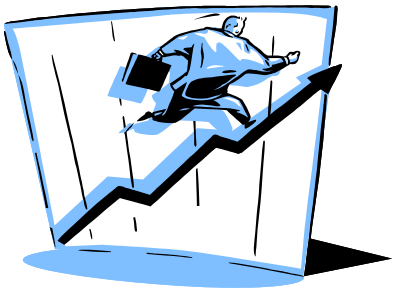
- *Impacto (impact)*: conseqüências de um incidente de segurança.

- *Risco (risk)*: combinação da probabilidade da concretização de uma ameaça e suas conseqüências.

- *Vulnerabilidade (vulnerability)*: fragilidade ou limitação de um ativo que pode ser explorada por uma ou mais ameaças.

OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

- Proteção da informação contra vários tipos de ameaças para garantir:



  - Continuidade do negócio
  - Minimização do risco ao negócio
  - Maximização do retorno sobre os investimentos
  - Oportunidades de negócio

ABNT NBR ISO/IEC 17799:2005

Qualquer tipo de informação deve ser protegido, esteja ele escrito ou desenhado em papel, armazenado em meios magnéticos, em filmes ou falado.

"A segurança da informação é obtida através da implantação de controles adequados, políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware."

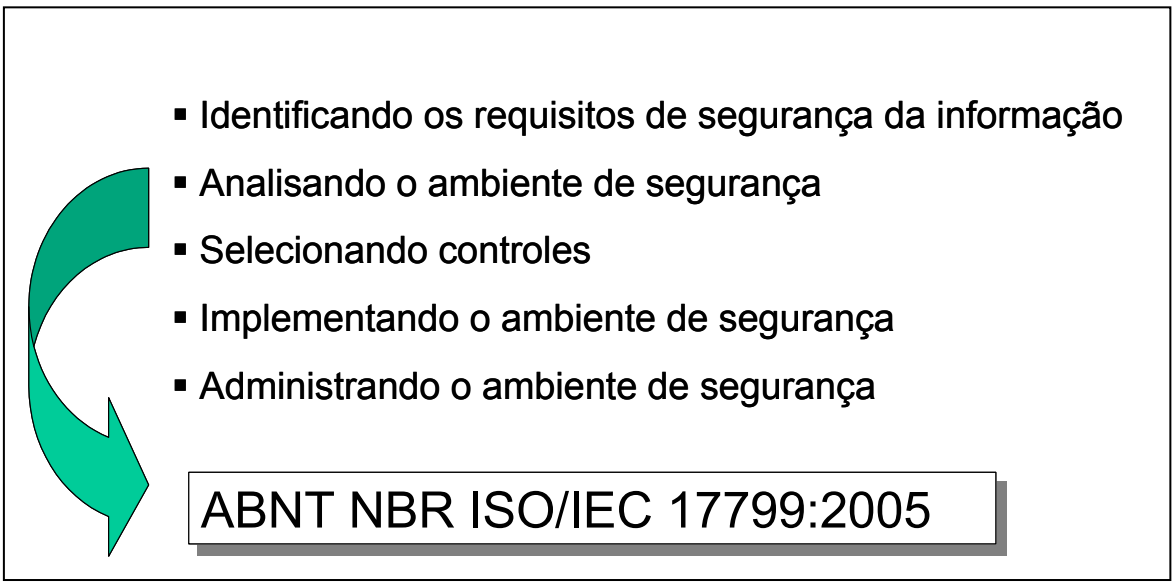
O objetivo da segurança da informação é garantir o funcionamento da organização frente às ameaças a que ela esteja sujeita.

A norma ABNT NBR ISO/IEC 17799:2005 "estabelece diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização". Essa frase confirma que a norma está alinhada com os objetivos de todas as outras normas criadas com o mesmo fim, conforme visto no capítulo 2.

É consenso das normas da área que os objetivos gerais da segurança da informação visam preservar a confidencialidade, integridade e disponibilidade da informação. Esse é um conceito da antiga ISO/IEC 17799:2000. Porém, é citado nesse curso por se tratar de um conceito amplamente difundido.

- *Confidencialidade*: tem o objetivo de garantir que apenas pessoas autorizadas tenham acesso à informação. Essa garantia deve ser obtida em todos os níveis, desde a geração da informação, passando pelos meios de transmissão, chegando a seu destino e sendo devidamente armazenada ou, se for necessário, destruída sem possibilidade de recuperação. Esse processo tende a ser mais dispendioso, quanto maior for a necessidade de proteção da informação e, é claro, quanto maior for o valor da informação a ser protegida. Modernos processos de criptografia aliados a controles de acesso são necessários nessa etapa.
- *Integridade*: O objetivo da integridade é garantir que a informação não seja alterada, a não ser por acesso autorizado. Isso significa dizer que uma informação íntegra não é necessariamente uma informação correta, mas sim que ela não foi alterada em seu conteúdo. Esse processo é a proteção da informação contra modificações não autorizadas ou acidentais.
- *Disponibilidade*: Garantir que a informação sempre poderá ser acessada quando for necessário. Esse objetivo é conseguido através da continuidade de serviço dos meios tecnológicos, envolvendo políticas de backup, redundância e segurança de acesso. De nada adianta ter uma informação confiável e íntegra se ela não está acessível quando solicitada.

A ABNT NBR ISO/IEC 17799:2005 amplia o conceito acima enfatizando mais os resultados da implantação de um ambiente de segurança da informação, quando define que “segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.



Um processo de planejamento de gestão e monitoramento de segurança de TI pode variar muito em uma organização. Devido aos diferentes estilos, tamanho e estrutura das organizações, o processo deve se adequar ao ambiente em que será usado. Alguns passos em linhas gerais são apresentados a seguir:

1. *Identificar os requisitos de segurança da informação*. Basicamente, existem três fontes principais para obtenção dos requisitos de segurança da informação:
   - Análise/avaliação de riscos para a organização.
   - Legislação vigente a que a organização, seus parceiros comerciais e provedores de serviço devem atender.
   - Princípios, objetivos e requisitos do negócio.

2. *Análise do ambiente de segurança*. É o levantamento periódico dos riscos de segurança da informação, identificando as ameaças e vulnerabilidades. Os resultados desse passo irão direcionar a determinação das ações gerenciais que nortearão todo o processo de segurança da informação.

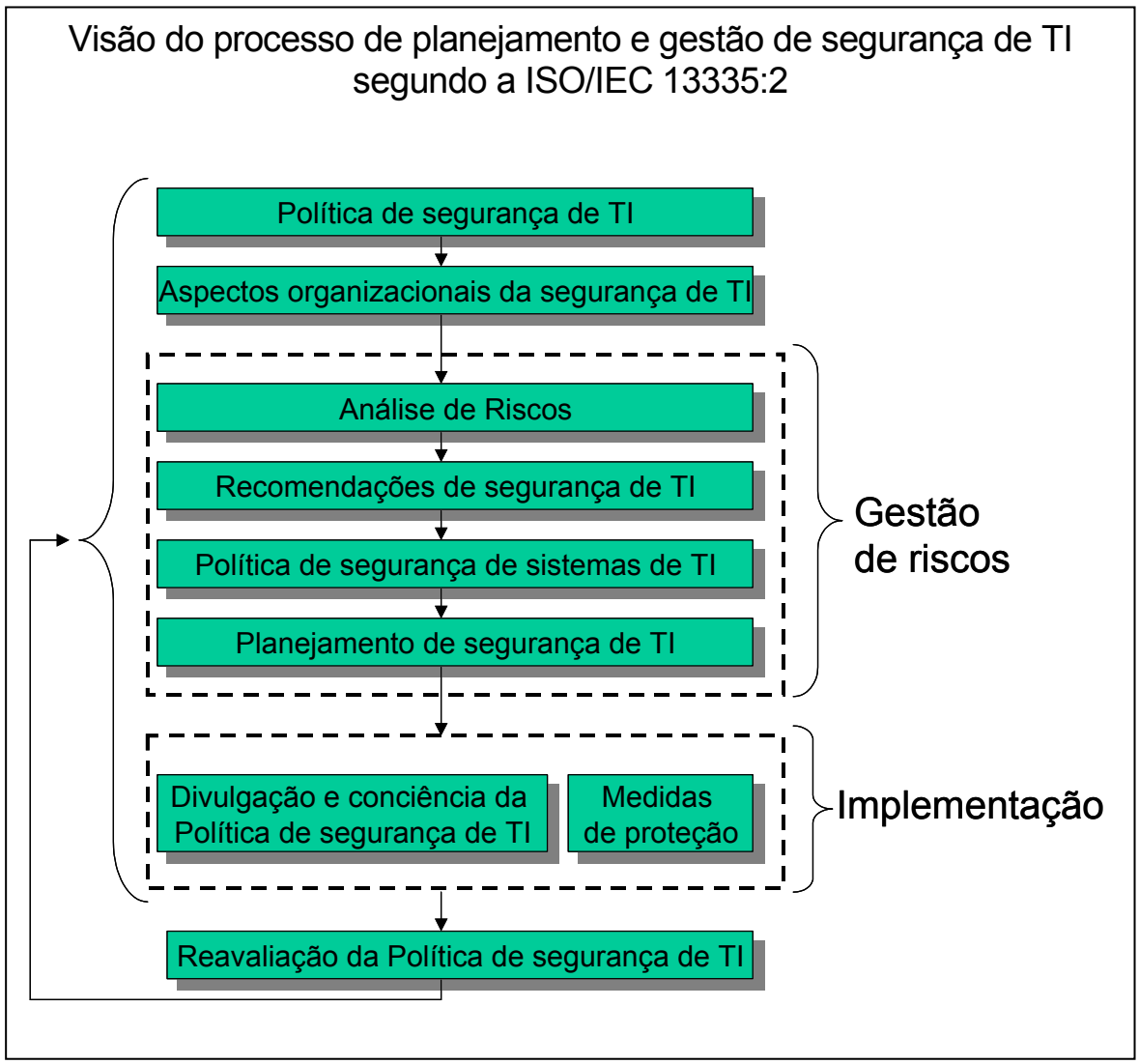
3. *Seleção de controles*. Com os riscos identificados e com as medidas de tratamento desses riscos já providenciadas agora é necessário implementar controles que assegurarão a redução dos riscos a níveis aceitáveis. A seleção de controles pode ser feita a partir dessa norma ou de outra que atenda as necessidades da organização. Esses controles incluem:
   - Proteção de dados e privacidade de informações pessoais;
   - Proteção dos registros organizacionais;
   - Direitos de propriedade intelectual;
   - Documento de política de segurança da informação;
   - Atribuição de responsabilidades;
   - Treinamento e educação em segurança da informação;
   - Processamento correto nas aplicações a fim de prevenir erros, perdas, modificação não autorizada ou mau uso de informações em aplicações;
   - Gestão de vulnerabilidades técnicas;
   - Gestão de continuidade de negócios;
   - Gestão de incidentes de segurança e melhorias.

4. *Implementação do ambiente de segurança*. Consiste em:
   - Criação, educação e disseminação interna da política de segurança da informação para todos os envolvidos;
   - Uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação;
   - Comprometimento de todos os níveis gerenciais;
   - Provisão de recursos financeiros para as atividades de gestão da segurança da informação.

5. *Administração do ambiente de segurança*. Inclui:
   - Estabelecimento de um processo de gestão de incidentes de segurança;
   - Implementação de um sistema de medição, que colha dados para a avaliação de desempenho da gestão de segurança;
   - Obtenção de sugestões de melhorias;
   - Implementação de melhorias levantadas no processo.

Um fluxograma mais detalhado das fases do processo é proposto pela norma ISO/IEC 13335-2 - Information technology — Guidelines for the management of IT

Security — Part 2: Managing and Planning IT Security. Essa norma é citada na ABNT NBR ISO/IEC 17799:2005 como informações adicionais para o processo de implantação da segurança de TI. O fluxograma reproduzido abaixo deixa claro que os trabalhos devem ser iniciados a partir dos objetivos de mais alto nível da empresa, ou seja, os negócios, e segue passando por definições de estratégia de segurança de TI até a elaboração de uma política de segurança de TI. É importante que todas as atividades sejam tratadas dentro do estilo e maneira da organização realizar negócios.



Capítulo

2

2 – ANÁLISE/AVALIAÇÃO E TRATAMENTO DE RISCOS

GERENCIAR SEGURANÇA DE TI INCLUI A ANÁLISE E AVALIAÇÃO DE RISCOS E COMO REDUZÍ-LOS A UM NÍVEL ACEITÁVEL. É NECESSÁRIO LEVAR EM CONTA OS OBJETIVOS DA ORGANIZAÇÃO, BEM COMO AS NECESSIDADES ESPECÍFICAS DE CADA SISTEMA E SEUS RISCOS.

NESTE CAPÍTULO VEREMOS COMO FAZER UMA AVALIAÇÃO DE RISCOS E COMO MINIMIZÁ-LOS.

OBJETIVO

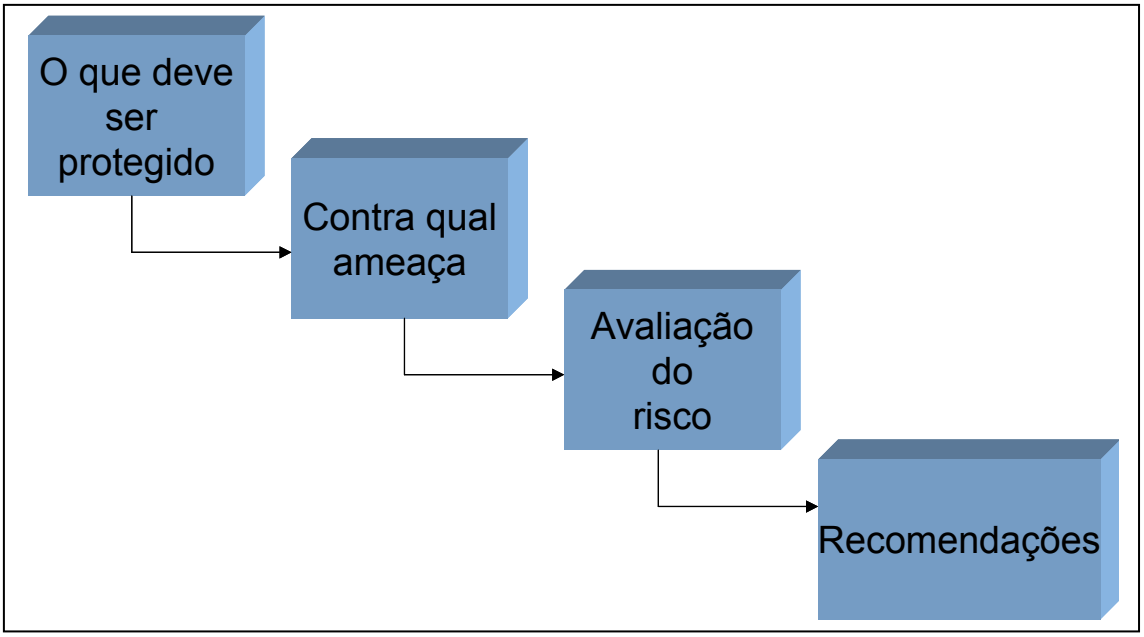
Sistemas de informação estão constantemente sujeitos a riscos provenientes de ações maliciosas, acidentes ou erros inadvertidos de usuários.

Avaliar os riscos potenciais e tomar ações para minimizá-los, é tarefa de uma gestão de segurança da informação.

Neste capítulo serão abordadas as melhores práticas para avaliação de riscos e como tratá-los.

Ao final deste capítulo você estará apto a:

- ❒ Identificar, quantificar e priorizar os riscos;
- ❒ Determinar ações de gestão apropriadas para o gerenciamento dos riscos de segurança da informação;
- ❒ Estabelecer os critérios de aceitação dos riscos;
- ❒ Tomar decisões sobre o tratamento dos riscos.



Segundo as definições da norma, risco é a "*combinação da probabilidade de um evento e de suas conseqüências*".

Por evento de segurança da informação, entenda-se uma "*ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação, ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação*". O evento é então a concretização de uma ameaça, que por sua vez é a "*causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização*".

Portanto, avaliar riscos, passa pela avaliação de ameaças e vulnerabilidades.

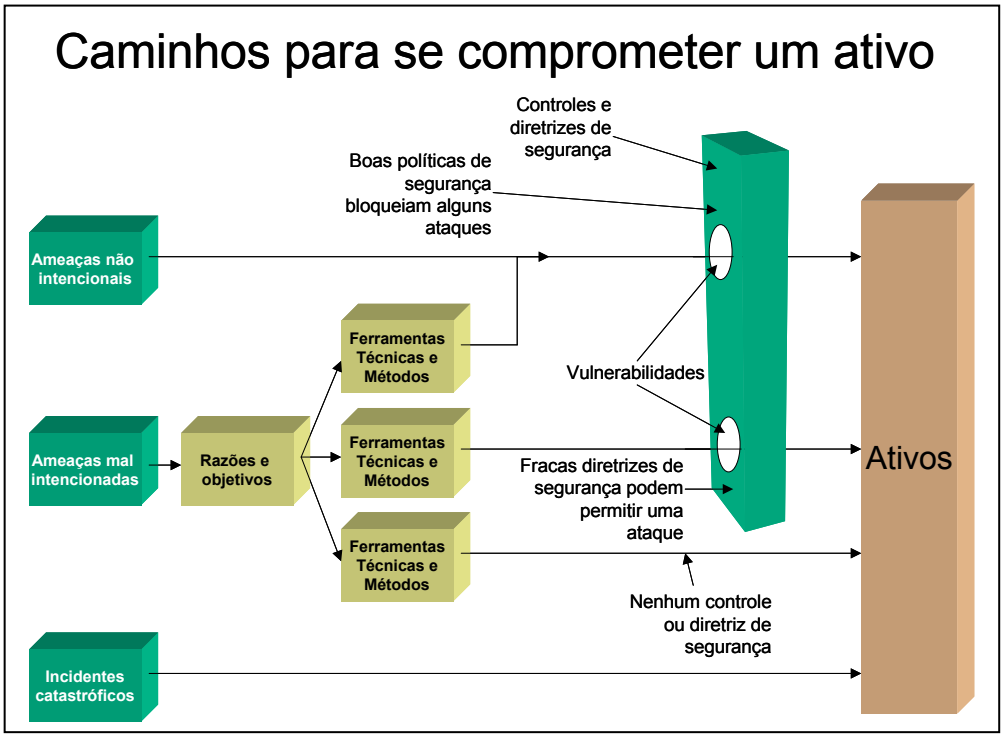
O principal desafio à segurança da informação das organizações é identificar e qualificar os riscos e ameaças às suas operações. Este é o primeiro passo no desenvolvimento e gerenciamento de um efetivo programa de segurança. Identificar os riscos e ameaças mais significantes tornará possível determinar ações apropriadas para reduzi-los.

Uma vez identificados, os riscos devem ser qualificados para que sejam priorizados em função de critérios de aceitação de riscos e dos objetivos relevantes para a organização. Esta atividade é apenas um elemento de uma

série de atividades de gerenciamento de riscos, que envolvem implementar políticas apropriadas e controles relacionados, promover a conscientização das medidas, e monitorar e avaliar políticas e controles efetivos.

A avaliação de riscos e ameaças não resulta em uma seleção de mecanismos de prevenção, detecção e resposta para redução de riscos. Ao contrário ela simplesmente indica as áreas onde esses mecanismos devem ser aplicados, e a prioridade que deve ser designada para o desenvolvimento de tais mecanismos. No contexto de gerenciamento de riscos, a avaliação de riscos e ameaças irá recomendar como minimizar, prevenir e aceitar os riscos.

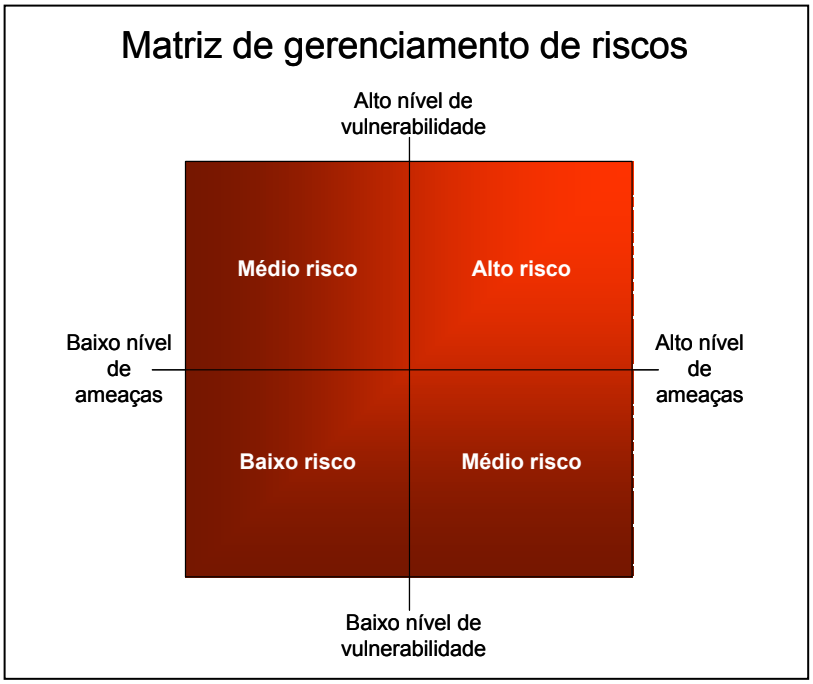
Como os riscos e ameaças podem mudar com o passar dos tempos, é importante que a organização periodicamente reavalie os mesmos e reconsidere as políticas e controles selecionados.



Existem vários caminhos que podem comprometer um ativo, conforme o nível de contramedidas implementadas. A figura acima dá uma idéia de que não há segurança totalmente garantida, mas sim implementações sujeitas a falhas. Isso não deve ser desanimador, pois implementar algumas contramedidas é melhor do que não implementar nenhuma. A avaliação de riscos visa exatamente determinar se as contramedidas existentes são suficientes ou não.

Independente do tipo de risco a ser considerado, uma avaliação de riscos geralmente inclui os seguintes passos:

- Identificar ameaças que podem causar danos e afetar os ativos e operações críticas. Ameaças incluem itens como intrusões, crimes, empregados insatisfeitos, terrorismo e desastres naturais;
- Estimar a probabilidade da concretização das ameaças, baseado em informações históricas e julgamento de conhecimentos individuais;
- Identificar e qualificar o valor, susceptibilidade e criticidade da operação e do ativo que poderá ser afetado se a ameaça se concretizar, a fim de determinar quais operações e ativos são mais importantes;
- Identificar o custo das ações para eliminar ou reduzir o risco. Isto poderá incluir a implementação de novas políticas organizacionais e procedimentos, bem como controles físicos ou técnicos;
- Documentar os resultados e desenvolver planos de ação.



O nível de riscos à segurança da informação aumenta conforme aumenta o nível das ameaças e vulnerabilidades, como pode ser visto na matriz de gerenciamento de riscos [1] acima.

O nível do risco existente em uma organização pode ser categorizado como:

- **Alto**: requer imediata atenção e implementação de contramedidas;
- **Médio**: Requer atenção e implementação de contramedidas em um futuro próximo;
- **Baixo**: Requer alguma atenção e consideração para implementação de contramedidas como boas práticas de negócios.

Cada ameaça e vulnerabilidade identificada também deve ser qualificada. Essa qualificação varia conforme a organização e o departamento. Por exemplo, a ameaça de enchente preocupa muito mais organizações instaladas nas proximidades de rios do que aquelas instaladas em regiões áridas. Danos causados a banco de dados de pesquisas de marketing podem ser menos danosos do que se causados a informações relativas ao fluxo financeiro da organização.

Os níveis de qualificação das ameaças podem ser assim definidos:

- ***Não aplicável***: significa que a ameaça considerada não é relevante para a situação examinada;
- ***Baixo***: não há histórico e considera-se que é improvável a concretização da ameaça;
- ***Médio***: significa que há algum histórico e probabilidade que a ameaça se concretize;
- ***Alto***: significa que há um histórico significante e uma avaliação de que a ameaça está por acontecer.

O objetivo da análise de riscos é identificar e avaliar os riscos e ameaças pelo qual o sistema de TI e seus ativos estão expostos, a fim identificar e selecionar contramedidas apropriadas.

A tabela da página seguinte [2] ilustra como a avaliação das informações de ameaças pode ser qualificada com base nos ativos que são colocados em risco.

A avaliação de ameaças conforme a tabela inclui:

a. Descrever as ameaças em termos de *quem*, *como* e *quando*;
b. Estabelecer em qual *classe de ameaça* a mesma se enquadra;
c. Determinar a *probabilidade* da concretização da ameaça;
d. Determinar as *conseqüências* nas operações do negócio caso a ameaça se concretize;
e. Calcular se o *impacto* das conseqüências leva a seqüelas pouco sérias, sérias ou excepcionalmente graves.
f. Calcular a *taxa de exposição* para cada ameaça, em termos da severidade relativa para a organização.

Ativo		Descreva o ativo
Avaliação da ameaça	**Agente / evento**	- Descreva a ameaça
	Classificação da ameaça	- ***Quebra de sigilo***: ameaça a confidencialidade da informação (Interceptação, manutenção imprópria, craker, procedimentos) - ***Interrupção***: ameaça a disponibilidade da informação (terremoto, fogo, inundação, código malicioso, falha de energia) - ***Modificação***: ameaça a integridade da informação (entrada errada de dados, códigos maliciosos, crakers) - ***Destruição***: terremoto, fogo, inundação, vandalismo, pico de energia) - ***Remoção ou perda***: ameaça a confidencialidade e disponibilidade (Roubo de dados ou sistemas em mídias portáteis como notebooks, Cds, disquetes)
	Probabilidade da ocorrência	- ***Baixo***: a ameaça nunca se concretizou e é pouco provável que ocorra - ***Médio***: há histórico de ocorrência e pode vir a ocorrer - ***Alto***: há histórico de ocorrência e grande probabilidade de ocorrer
	Conseqüência da ocorrência	Lista de conseqüências para a organização caso a ameaça se concretize: relata as perdas ou outras conseqüências caso a ameaça se concretize
	Impacto	Determinar o impacto para a organização em termos de custo associados com perda de confidencialidade, integridade e disponibilidade. O impacto pode ser: - ***Excepcionalmente grave*** - ***Sério*** - ***Pouco Sério***
	Taxa de exposição	Valor numérico de 1 a 9: - ***Excepcionalmente grave*****:** 7 a 9 - ***Sério***: 4 a 6 - ***Pouco Sério***: 1 a 3

A tabela a seguir, mostra um modelo genérico de avaliação de riscos e recomendações. Juntamente com a tabela anterior pode ser usado para auxiliar na tomada de decisão que deve ser tomada para o tratamento de cada risco identificado. Segundo a norma, possíveis opções de tratamento do risco incluem:

a. Aplicar controles apropriados para reduzir os riscos;
b. Conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à política da organização e aos critérios para aceitação de risco;
c. Evitar riscos, não permitindo ações que poderiam causar a ocorrência dos mesmos;
d. Transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Ativo		Descreva o ativo
Avaliação de riscos	**Contramedidas existentes**	DESCREVA: contramedidas existentes para combater a ameaça
	Vulnerabilidades	DESCREVA: as vulnerabilidades relacionadas com a ameaça
	Riscos	AVALIE os riscos como: - Baixo - Médio - Alto
Recomendações	**Contramedidas propostas**	RECOMENDA-SE: implementação de novas contramedidas ou remoção de contramedidas desnecessárias
	Riscos projetados	AVALIE: os riscos projetados como: - Baixo - Médio - Alto
	Avaliação de contramedidas	AVALIE AS CONTRAMEDIDAS COMO: - Completamente satisfatória - Satisfatória na maioria dos aspectos - Necessita melhoras

OBS: Existem algumas metodologias para avaliação de riscos. Com base em necessidades de negócios, o Centro de Excelência de Segurança (SCOE – Security Center Of Excelence) da Microsoft desenvolveu uma metodologia completa que pode ser encontrada em: http://www.microsoft.com/brasil/security/guidance/riscos/default.mspx ; ou na sua versão completa e

constantemente atualizada (em inglês) para download e contendo planilhas para ser utilizada durante a análise, em: http://go.microsoft.com/fwlink/?linkid=32050

Capítulo

3

3 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

NESTE CAPÍTULO VEREMOS COMO CRIAR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

OBJETIVO

Escrever uma política de segurança da informação envolve comprometimento de diversas áreas de interesse e deve ser abraçada por todos, desde a direção da organização até cada um dos funcionários, clientes e fornecedores com acesso ao sistema de informação, ou que possam de alguma forma comprometer o ativo protegido.

O documento de política de segurança da informação deve ser elaborado de forma a servir como uma regra a ser seguida. Constantemente exigirá atualizações que reflitam as necessidades do negócio e a realidade da organização.

Neste capítulo veremos como criar e organizar uma política de segurança da informação nas organizações.

Ao final deste capítulo você estará apto a:

- ❒ Conceituar o que é uma política de segurança da informação;
- ❒ Fazer uma análise crítica da política de segurança da informação;
- ❒ Estabelecer uma criteriosa política de segurança da informação conforme os requisitos do negócio;
- ❒ Entender os documentos requeridos para a implantação e divulgação da política de segurança da informação;

- "*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"*

- É preferível uma política mal escrita a nenhuma política.

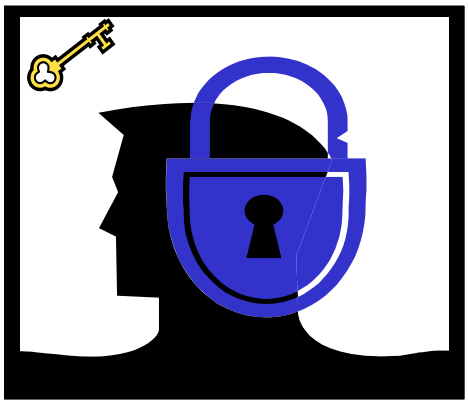
Segundo a norma ABNT NBR ISO/IEC 17799:2005, uma política de segurança da informação visa "*Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes"*, ou seja, ela propõe uma política que sistematize um processo a fim de minimizar as preocupações da direção com a segurança de seus ativos.

Escrever uma política é uma tarefa muitas vezes difícil e deve contar com o envolvimento de várias pessoas, de vários departamentos. Isso não deve ser desanimador e não se deve procrastinar o início dos trabalhos, haja vista a fragilidade a que o negócio pode estar exposto.

Se necessário, para implementar e manter esta política, deverá ser utilizada consultoria especializada, com conhecimento nos diversos aspectos da segurança dos bens de informação e das tecnologias que os apóiam.

Possuir uma política de segurança da informação na organização é importantíssimo para o sucesso dos negócios. É preferível uma política mal escrita a nenhuma política.

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política de segurança
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. Refaça o processo

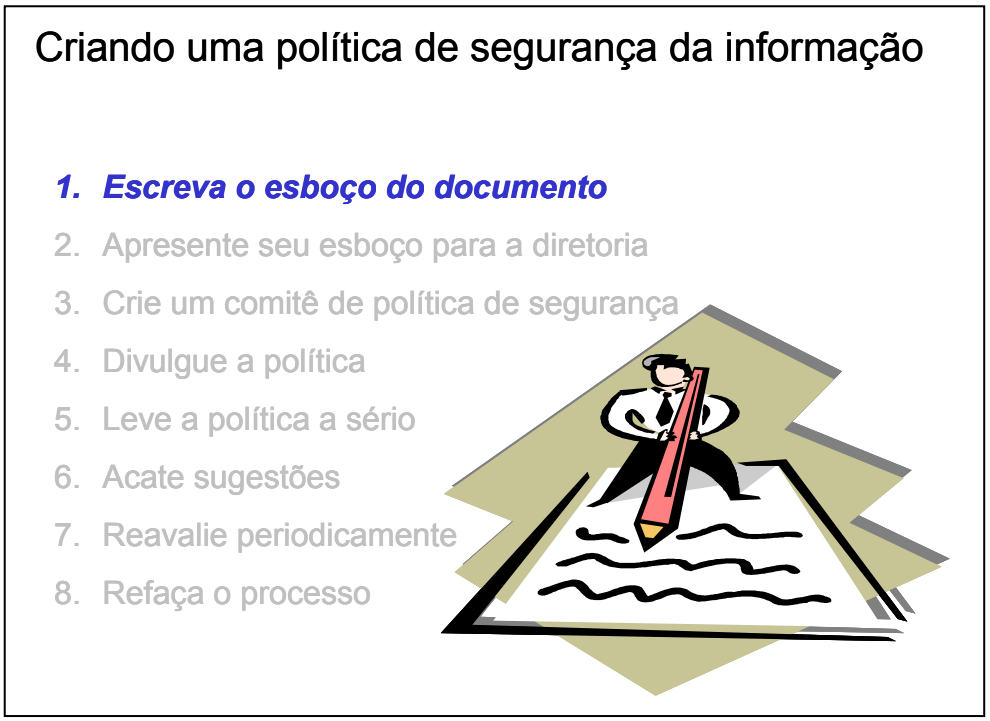


O primeiro passo para a criação de uma política de segurança da informação é ter alguém responsável por ela. Deve haver uma área responsável pela política de segurança da informação, que se incumbirá de sua criação, implantação, revisão, atualização e designação de funções. Nessa área deve ser escolhido um gestor responsável pela análise e manutenção da política. Para garantir a aplicação eficaz da política, o ideal é que o alto escalão, como diretoria, gerentes e supervisores façam parte dessa área, além de usuários, desenvolvedores, auditores, especialistas em questões legais, recursos humanos, TI e gestão de riscos.

Thomas A. Wadlow [**Error! Bookmark not defined.**], propõe um processo para se estabelecer uma política que prevê a possibilidade de implantação imediata na organização sem muita delonga. A princípio o processo não requer o engajamento imediato da direção, que, aos poucos deverá ser incluída. Essa abordagem, leva em consideração a experiência na implantação do processo da política.

Como a norma é explícita no comprometimento da direção, neste curso adotaremos uma abordagem adaptada de Thomas A. Wadlow como o ponto de partida para a tarefa de implantação da política de segurança da informação. Vamos supor que você leitor foi escolhido como o responsável pela implantação

da política de segurança da informação. Siga os passos abaixo para dar início aos trabalhos o quanto antes:



1. ***Escreva o esboço do documento da política de segurança para sua organização***. Esse documento deve ser genérico, possuir apenas suas idéias principais, sem preocupação com precisão. Não deverá possuir mais do que 5 páginas. Escreva também uma justificativa para sua implantação, sempre com o foco nos negócios e riscos a que a organização está sujeita caso não se implante a política de segurança da informação.

   Procure fazer um documento com foco nos processos de negócio, e não na tecnologia. Para obter o apoio da diretoria é necessário que se mostre qual operação está em risco.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. ***Apresente seu esboço para a diretoria***
3. Crie um comitê de política de segurança
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. Refaça o processo

2. ***Apresente seu esboço para a diretoria***. O objetivo é angariar a confiança no projeto e o engajamento da direção. Uma vez que ela esteja convencida da importância da política, você terá carta branca para a o início da implantação.

   O apoio da diretoria é fundamental para o sucesso da política de segurança. Em algumas situações somente com o apoio da diretoria será possível aplicar as políticas criadas.

   A diretoria, ou alta gestão, é conhecida no processo de política de segurança como patrocinador (ou sponsor), pois seu apoio garante que é uma decisão válida para toda a organização.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. ***Crie um comitê de política de segurança***
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. Refaça o processo

3. ***Crie um comitê de política de segurança***. Esse comitê deverá ser formado por pessoas interessadas na criação da política de segurança e devem ser de setores distintos na organização. Com base em seu documento, a função do comitê será:

    a. escrever as regras para a política;
    b. definir atribuições;
    c. detalhar os procedimentos bem como as penas para violações da mesma;
    d. aprovar as normas estipuladas e alterações propostas.

    O comitê terá a função legisladora do processo. Porém, continua sendo sua a responsabilidade pela aplicação da política. O comitê deverá se reunir pelo menos uma vez a cada três meses e, extraordinariamente, se houver necessidade. A reunião tem o objetivo de avaliar e aprimorar a política de segurança, os incidentes ocorridos e as ações tomadas para correção.

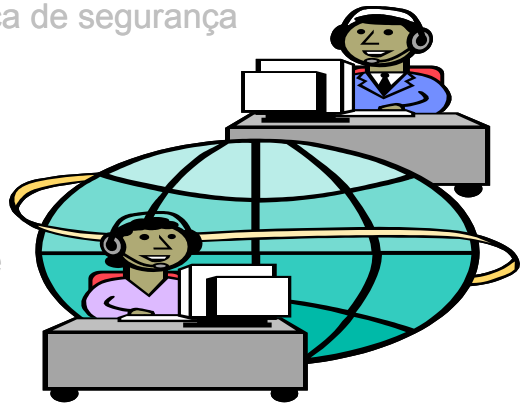
    O documento criado por você, juntamente com o comitê, deverá ter uma linguagem simples a fim de que todos os usuários a entendam e possam aplicá-la com facilidade. Assim, para que a política de segurança da informação seja eficaz, o documento será na verdade, um conjunto de políticas inter-relacionadas. A partir deste momento, você já terá em mãos um documento oficial que deverá ser aceito e aprovado pela direção. Dependendo da natureza da organização esse documento tende a ser

muito extenso com dezenas ou centenas de páginas.

Embora a formação do comitê varie de organização para organização, procure envolver (sempre que possível) pessoas de diversas áreas, com diversas visões, sendo assim, é importante a participação de pessoas da área de Auditoria, Jurídico, Recursos Humanos e de Associações de classe, além de tecnologia. Desta forma um maior número de pontos de vistas e interesses serão levados em consideração, garantindo maior transparência e abrangência.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política de segurança
4. ***Divulgue a política***
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. Refaça o processo



4. ***Divulgue a política de segurança da informação***. A política deve ser de conhecimento de todos e compreensível para todos que interagem com a organização, usuários internos e externos.

   Deve sempre estar nas mãos de quem vai utilizá-la. Porém, de nada vale colocar o documento inteiro nas mãos de quem vai utilizar apenas uma parte.

   Um funcionário da limpeza precisa saber como limpar um determinado equipamento preservando a integridade física do mesmo. Caso veja, por exemplo, um fio desencapado, deve saber a quem avisar para solucionar o incidente. Um funcionário da contabilidade precisa saber sua senha para acessar o banco de dados pertinente ao seu setor. Precisa saber também a quem recorrer caso precise acessar dados antigos, armazenados em fita, e que precisam ser restaurados. Porém, não precisa saber os detalhes de como são realizados os backups.

   A divulgação eficaz é aquela que atinge a pessoa certa com a informação que ela precisa saber. Ela não precisa ler toda a política de segurança, mas a parte que lhe interessa. Essa divulgação segmentada é fator imprescindível para o sucesso da empreitada. É claro que isso não exclui a necessidade de divulgação de todo o documento caso alguém se interesse em lê-lo.

   Uma forma prática de divulgação é a criação de um Web site na intranet da empresa. Nele todas as informações sobre a política devem ser bem

redigidas e separadas em seções, facilitando o acesso a políticas gerais às quais todos devem obedecer e a políticas específicas para cada setor. Este site servirá de repositório de tudo o que for estabelecido na política e servirá também para coletar sugestões.

Outras formas de divulgação também poderão ser usadas como um fórum, e-mails periódicos, ferramentas colaborativas de troca de informação.

Se a política de segurança da informação for divulgada fora da organização, tome o cuidado de não revelar informações sensíveis. Lembre-se de classificar as informações sigilosas para acesso apenas a pessoas específicas.

5. ***Trate a política e as emendas como regras absolutas com força de lei***. Uma vez que a política já é do conhecimento de todos, não pode haver violações da mesma. Caso isso ocorra, devem ser previstos procedimentos que vão de advertências a punições. As violações devem ser analisadas em suas causas, conseqüências e circunstâncias, a fim de que sejam tomadas medidas preventivas e corretivas que alterem a política para evitar nova situação de vulnerabilidade. Lembre-se que tudo deve ser documentado.

   Neste ponto, o apoio da diretoria tratado nos itens 1 e 2 é fundamental para que se possa cumprir as punições previstas na política. Caso estas deixem de ser cumpridas a política perde sua credibilidade e força junto aos demais colaboradores da organização.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política de segurança
4. Divulgue a política
5. Leve a política a sério
6. ***Acate sugestões***
7. Reavalie periodicamente
8. Refaça o processo

6. ***Sugestões são sempre bem-vindas***. Incentive que os colaboradores proponham sugestões de melhorias. Todas devem ser levadas em consideração. As pessoas que estão na rotina do trabalho, são as que mais estão aptas a levantar problemas de segurança na respectiva área, ou mesmo provocá-los.

   Algumas sugestões podem mostrar também que a política possui um rigor exagerado em determinado item, o que pode tornar seu cumprimento demasiadamente oneroso. Neste caso devemos analisar as críticas e estudar uma forma alterá-las ou criar tratamento de exceções para garantir o cumprimento das normas.

   Facilite o canal de comunicação para que as sugestões cheguem ao comitê. As sugestões pertinentes deverão virar emendas à política.

Criando uma política de segurança da informação

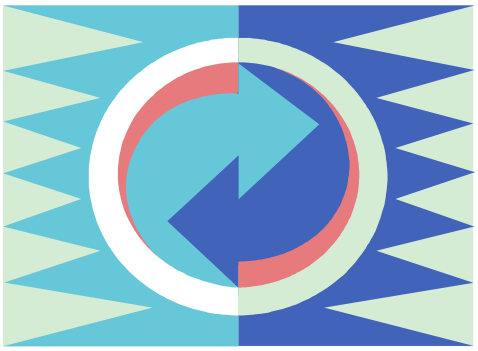
1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política de segurança
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. ***Reavalie periodicamente***
8. Refaça o processo

7. ***Realize reuniões periódicas para consolidar a política e as emendas***. Essas reuniões deverão ocorrer pelo menos uma vez ao ano. Deverão participar todo o comitê de política de segurança, a direção, e os responsáveis com funções delegadas. O objetivo é realizar uma análise crítica da política de segurança vigente, das emendas e dos incidentes relatados. Esta avaliação poderá gerar um documento atualizado que inclua todas as alterações.

   Neste ponto devemos considerar as sugestões levantadas no item 6 e todas as alterações do ambiente desde a última reunião, bem como mudanças na legislação, para que sirvam como base para o processo de revisão.

Criando uma política de segurança da informação

1. Escreva o esboço do documento
2. Apresente seu esboço para a diretoria
3. Crie um comitê de política de segurança
4. Divulgue a política
5. Leve a política a sério
6. Acate sugestões
7. Reavalie periodicamente
8. ***Refaça o processo***



8. ***Refaça o processo***. A nova declaração gerada no passo 7 deverá passar por todo o processo novamente, a fim de que entre em vigor e seja do conhecimento de todos.

Todos os 8 passos apresentados não são fáceis e envolvem muito trabalho, porém criam uma metodologia por etapas que, uma vez seguida, levará ao sucesso da criação da política de segurança da informação.

CONTEÚDO DO DOCUMENTO FORMAL DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O conteúdo do documento elaborado para a política de segurança da informação varia de uma organização para outra, em função de sua maturidade, disponibilidade de recursos, necessidades do negócio, área de atuação, etc... Deve ser simples, objetivo e compreensível para todos.

O Documento consta normalmente de:

a. ***Definição de segurança da informação, metas, escopo e importância da segurança da informação como mecanismo que possibilita o compartilhamento da informação***. Esse item é um texto explicativo do que é segurança da informação, como o texto apresentado no capítulo 3, subitens "Conceitos básicos de Segurança da Informação" e "Objetivos da Segurança da Informação".

b. ***Declaração do comprometimento da direção apoiando metas e princípios***. Mais uma vez, uma etapa bem simples de ser executada. Pode ser apenas uma frase assinada pela direção, como por exemplo:

   "A Diretoria da XYZ S/A declara-se comprometida em proteger todos os ativos ligados à Tecnologia da Informação, apoiando as metas e princípios da segurança da informação estabelecidas neste documento, a fim de garantir a confiabilidade, disponibilidade e integridade da informação,

alinhada com as estratégias do negócio".

O importante nesse item é que a assinatura da direção realmente expresse a vontade e engajamento do alto escalão da empresa, apoiando ativamente as ações a serem implantadas e definindo atribuições de forma explícita.

c. ***Estrutura para estabelecer objetivos de controles e controles, incluindo estrutura e análise/avaliação e gerenciamento de risco.*** Veja o capítulo 4.

d. ***Princípios de conformidade com a legislação e regulamentos contratuais***. Aqui deve ser avaliada a questão legal do negócio, suas conformidades com a legislação vigente e com regulamentos e contratos. As cláusulas do documento de política de segurança da informação devem estar em conformidade com essa avaliação. Por exemplo, caso a organização seja uma entidade pública, ela está obrigada a obedecer uma política de segurança conforme o decreto presidencial nº 3.505.

e. ***Plano de treinamento em segurança da informação***. É muito importante que todos os envolvidos com a segurança da informação, tenham não só acesso ao documento de política, como também sejam instruídos no processo de implantação e uso da política. Tendo conhecimento e formação adequada, a eficácia do plano de segurança terá mais chances de sucesso. Além disso, todos passam a ser co-responsáveis pelo processo uma vez que não podem alegar desconhecimento do mesmo. O treinamento poderá ser feito, por exemplo, através de seminários programados, distribuições de cartilhas com informações sobre a segurança da informação, e-mails regulares com dicas sobre o assunto e site de divulgação da política.

f. ***Plano para gestão de continuidade do negócio***. É um conjunto de estratégias e procedimentos que visam garantir que não haverá interrupção das atividades do negócio, além de proteger os processos críticos no caso de alguma falha. É um conjunto de medidas que combinam ações preventivas e de recuperação.

g. ***Conseqüência das violações na política de segurança***. É necessário que todos saibam das conseqüências da violação na política. Essas conseqüências passam por punições que devem ser explicitadas no documento. O responsável pela aplicação da política deve estar bem preparado para a eventualidade de ter que, por exemplo, solicitar a

demissão de um bom funcionário que tenha violado a política. Isso pode ser constrangedor, mas necessário. Por isso, explicite e divulgue bem essa parte para evitar desculpas de desconhecimento das normas.

h. ***Definição das responsabilidades na gestão da segurança***. A designação das "responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança da informação específicos devem ser claramente definidas". Essa é uma atribuição do comitê gestor da política. Para que haja o comprometimento dos responsáveis, pode ser criado um termo de responsabilidade e sigilo que compromete os envolvidos, internos e externos com a política de segurança da organização. Esses responsáveis podem delegar tarefas de segurança da informação para outros usuários, porém continuam responsáveis pela mesma.

i. ***Referências à documentação que apóiam a política***. Esta parte do documento serve para fortalecer ainda mais a política, indicando documentos complementares que detalham procedimentos de sistemas implantados ou regras a serem seguidas.

Capítulo

4

4 – ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

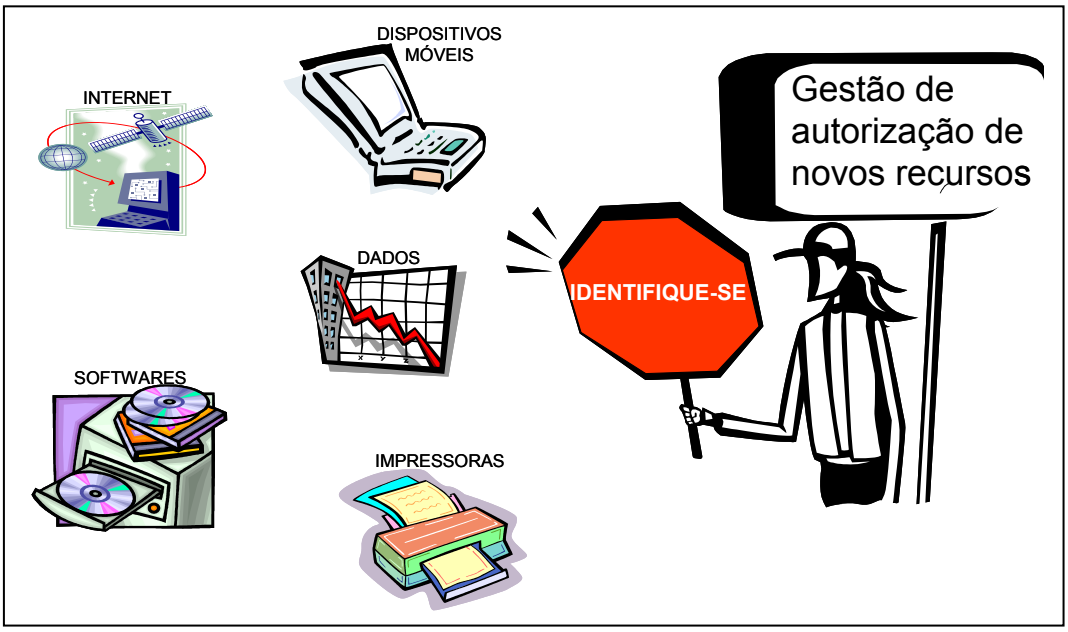
NESTE CAPÍTULO VEREMOS ALGUNS ASPECTOS COMPLEMENTARES SOBRE COMO ORGANIZAR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

OBJETIVO

Neste capítulo veremos alguns aspectos complementares para a organização de uma política de segurança da informação.

Ao final deste capítulo você estará apto a:

- ❒ Entender a importância do gerenciamento de autorização de novos recursos;
- ❒ Porque criar acordos de confidencialidade;
- ❒ Lidar com informações sigilosas quando a operação envolve serviços de terceiros.



Autorizar o acesso a novos recursos de processamento de informação é uma tarefa rotineira de um administrador de rede, que exerce a função de administrador de usuários. A cada momento alguém solicita acesso a uma impressora específica ou informações de um banco de dados, ou a qualquer outro recurso.

Para autorizar acessos aos recursos, o administrador deve ter em mãos um processo de gestão que seja compatível com a política de segurança. Esse processo definirá quem poderá ter acesso a um recurso. Isso pode ser obtido, por exemplo, através de controles lógicos de acesso. Estes têm o objetivo de impedir acessos não autorizados, protegendo os equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

O processo de gestão de autorização de novos recursos, também deve prever a verificação de compatibilidade de softwares e hardwares com o sistema.

Dispositivos móveis devem ter atenção especial, uma vez que podem introduzir novas vulnerabilidades. Como a maioria dos dispositivos móveis como os PDAs e os notebooks, já vêem de fábrica com interfaces sem fio (wireless) instalada, e como mesmo os dispositivos como placas de redes sem fio e pontos de acesso

(access point) são hoje dispositivos do tipo plug & play (conecte e use), eles criam um portal de entrada à rede caso configurações de segurança não sejam adequadamente executadas.

Dispositivos sem fio estão cada vez mais populares e seus benefícios para o usuário são inegáveis. Porém, as empresas têm de criar processos de segurança específicos que as protejam, como procedimentos de autenticação de usuários, sistemas de varredura para detecção de pontos de acesso clandestinos (muitas vezes conectados à rede inocentemente por um funcionário que deseja usufruir a mobilidade) e inclusão de todos os equipamentos em um serviço de diretório.

Acordos de confidencialidade e restrições de acesso

- Objetivo: Proteger todo conhecimento técnico ou informação confidencial contra divulgação não autorizada por:
  - Funcionários;
  - Ex-funcionários;
  - Terceirizados;
  - Partes externas;
  - Clientes.

Segurança é um problema que envolve principalmente pessoas, mais até do que aspectos físicos ou aspectos tecnológicos. Por isso, é necessário que haja procedimentos específicos que tratem com cuidado as pessoas que têm acesso às informações da organização. Um dos grandes riscos para segurança da informação, é a quebra de sigilo das informações por parte de funcionários contratados ou terceirizados e partes externas. Essa quebra de sigilo pode ocorrer intencionalmente ou não. Um funcionário pode comentar uma informação em simples conversas informais em uma mesa de bar ou no saguão do aeroporto. Essa conversa pode ser ouvida por um concorrente que se beneficiará da informação.

Outro risco é o ex-funcionário insatisfeito que divulga a terceiros, informações cruciais da organização, ou que já sabendo de sua demissão, toma alguma ação que viole a segurança interna.

Para tentar coibir essas ações, o responsável pela política tem a obrigação de orientar um novo funcionário quanto à política de segurança e as devidas punições cabíveis, caso a mesma não seja cumprida.

Além de todas as medidas de segurança efetivas implantadas, é recomendável que sejam criados acordos de confidencialidade e sigilo das informações acessadas dentro da organização. Esses acordos devem seguir termos legais a fim de que tenham valor jurídico no caso de violação do mesmo.

O acordo de confidencialidade e sigilo deve ser bem explícito quanto à natureza do que se está protegendo. Tem o objetivo de proteger todo o conhecimento, técnico ou informação confidencial capaz de possibilitar seu emprego no processo produtivo econômico.

A proteção pretendida pelo acordo terá validade não só dentro do prazo de relação entre as partes, como também na ausência dele.

Eventualmente, dependendo do tipo de informação, o acordo de confidencialidade e sigilo poderá ser por tempo determinado, permitindo a divulgação do bem protegido ao fim daquele prazo ou em prazo previsto.

Empresas parceiras ou contratadas para um determinado serviço, também podem se beneficiar de informações sigilosas a que tenham acesso. Por isso, os acordos devem ser aplicados também a partes externas a organização.

Uma outra fonte de risco a ser analisada com relação a partes externas, é o acesso destes aos recursos de processamento da informação. Leve em consideração que produtos e serviços oriundos de partes externas podem reduzir a segurança da informação. Por exemplo, a permissão de acesso a Internet para o notebook de um visitante, deve ser feita com contas específicas com restrições de acesso a qualquer outro recurso da rede, pois uma vez conectado o visitante poderá explorar vulnerabilidades da rede, ou mesmo sem intenção, introduzir algum vírus no sistema.

Avalie todos os riscos potenciais que partes externas podem trazer e tome as contramedidas cabíveis. Por exemplo, o acesso físico a computadores por parte de um visitante ou contratado para um serviço, ou o acesso lógico deste a banco de dados, ou a uma conexão a rede, etc., só poderá ser feito com a autorização específica do responsável pela segurança de TI, o qual deverá permitir o acesso apenas aos recursos estritamente necessários ao trabalho a ser desempenhado.

O acesso de clientes e terceiros aos ativos ou às informações da organização também deve ser controlado e atender aos requisitos de segurança da

informação. Para isso, devem ser criados acordos com o cliente, os quais conterão todos os riscos identificados e os requisitos de segurança da informação. Também devem ser incluídos procedimentos de controles requeridos em um plano de gestão, como controle com identificadores únicos de acesso, através de usuário e senha, número de licença para ativação de software adquirido, etc.

Normas técnicas

1. ABNT NBR ISO/IEC 17799:2005 - Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. Associação Brasileira de Normas Técnicas (ABNT). Segunda edição, 2005.

2. ISO/IEC FDIS 17799:2005(E) – Information technology – Security techniiques - Code of practice for information security management. ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2005.

3. ISO/IEC 13335-2 - Information technology - Guidelines for the management of IT Security - Part 2: Managing and Planning IT Security. ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).

4. Information Technology Infraestructure Library (ITIL). Office of Government of Commerce (OGC), 1989.

5. CobiT (Control Objectives for Information and related Technology). ISACA (Information systems Audit and Control Foundation), 1996.

6. BS 15000:2000 - Specification for IT service management. British Standards Institution (BSI), 2000.

7. ISO/IEC 20000 - IT Service Management Standards. ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2005.

8. BS 7799 - Information security management – Part 1: Code of practice for Information security management. British Standard, 1999.

Referências

[1] www.microsoft.com/brasil/security/guidance/prodtech/win2000/secmod133.mspx#EDF.

[2] Guide to Threat and Risk Assessment for Information Technology – Security Information Publication 5 – IT Security of the RCMP – 1994.