Segurança da Informação

Aula 04

Política de segurança:

Qualquer organização sempre estabelece regulamentos políticos a serem seguidos por todos quantos se relacionem com ela.

Política de segurança é um conjunto de diretrizes gerais destinadas a governar a proteção a ser dada a ativos da companhia.

Aula 04

Segurança da Informação

As conseqüências de uma política de segurança implementada e corretamente seguida podem ser resumidas em três aspectos:

- Redução da probabilidade de ocorrências ;
- Redução dos danos provocados por eventuais ocorrências ;
- Criação de procedimentos para se recuperar de eventuais danos.

Aula 04

Segurança da Informação

Redução da probabilidade de ocorrências

As medidas de uma política de segurança devem ser de cunho preventivo.

Os eventuais riscos devem ser previstos e eliminados antes que se manifestem.

A prevenção costuma ser mais barata que a restauração dos danos provocados por falta de segurança.

De uma forma geral, as estruturas organizacionais conhecem os limites das atribuições e responsabilidade dentro de suas áreas de atuação e os riscos envolvidos.

As medidas de prevenção são, em princípio, essencialmente de cunho normativo.

Aula 04

Segurança da Informação

Redução dos danos causados por eventuais ocorrências

Se vier acontecer algum tipo de ocorrência danosa à segurança, os danos resultantes devem ser reduzidos ao mínimo.

As medidas de redução de riscos variam em função dos ativos e dos riscos envolvidos, e por este motivo as medidas são também de caráter mais normativo do que de procedimentos.

Aula 04

Segurança da Informação

Recuperação de danos provocados por ocorrências

É necessário haver um plano para recuperar os danos provocados pela ocorrência.

As medidas de recuperação dos danos também variam em função dos ativos e dos riscos envolvidos, geralmente, os procedimentos de recuperação dos danos confundem-se com o plano de contingência.

Aula 04

Segurança da Informação

A Cultura da organização

Todas as organizações humanas desenvolvem sua própria cultura interna, que governa os relacionamentos internos e externos.

Dentre todas as mudanças de cultura, uma das que mais sofrem resistência é a implantação de controles em uma estrutura. Segurança de informação não é exceção.

A disseminação da cultura de informática contribuiu para proliferação de “cursos de informática” de baixa qualidade, o que resultou na redução da qualidade média da mão-de-obra oferecida no mercado.

Aula 04

Segurança da Informação

A Cultura da organização

Além da menor competência técnica, há em determinadas empresas a se despedir mão-de-obra mais cara para se contratar uma mais barata.

O profissional de informática trabalha com informações, produto intimamente relacionado com a cultura específica de cada empresa.

A rotatividade de mão-de-obra nesta área, implica numa aculturação do “noviço” que dura algum tempo, podendo ocorrer pequenos erros que geram custos que nem sempre compensam na redução da folha de pagamento.

Aula 04

Segurança da Informação

O que deve constar da política de segurança

1. Identificar e definir o que se deseja, fixando-se objetivos a serem atendidos;
2. Identificar meios e recursos necessários;
3. Estabelecer etapas a cumprir e prazos das mesmas;

" (...) Ainda assim, o planejamento raramente atende a todas as situações que aparecem , de modo que, freqüentemente, há necessidade de acertar desvios de rota ou até mesmo mudar radicalmente o planejado originalmente. (...) "

Aula 04

Segurança da Informação

O que deve constar da política de segurança

Segurança também implica no uso de capital, mão-de-obra e recursos, isto é, representa investimento e despesas para a empresa.

Mas como se elabora uma política de segurança?
Qual é o nível de investimento necessário?
Qual o tamanho da equipe permanentemente alocada em segurança?
Qual deve ser o nível de segurança a ser implantada?
Qual a abrangência da segurança?
Deve-se contratar profissional externo ou treinar um interno?
Qual o perfil do profissional da pessoa responsável pela segurança – administrativo ou técnico?

Aula 04

Segurança da Informação

A política da segurança deve conter diretrizes claras a respeito, pelo menos, dos seguintes aspectos:

- Objetivo da segurança – deve explicar de forma rápida e sucinta a finalidade da política de segurança ;
- A quem se destina – deve definir claramente quais as estruturas organizacionais às quais a mesma se aplica ;
- Propriedade dos recursos – deve definir de forma clara as regras que regerão os diversos aspectos relacionados com a propriedade de ativos de informações ;
- Responsabilidades – deve definir de forma clara qual o tipo de responsabilidades envolvidas com o manuseio de ativos de informações, a quem as mesmas devem ser atribuídas e os mecanismos de transferência ;

Aula 04

Segurança da Informação

A política da segurança deve conter diretrizes claras a respeito, pelo menos, dos seguintes aspectos:

- Requisitos de acesso – deve indicar de forma clara quais os requisitos a serem atendidos para o acesso a ativos de informações ;
- Responsabilização – deve indicar as medidas a serem tomadas nos casos de infringência às normas da mesma ;
- Generalidades – nesta seção da política podem ser incluídos os aspectos que não cabem nas demais. Pode-se incluir aqui uma definição dos conceitos envolvidos, um glossário e uma indicação das normas acessórias.

Aula 04

Segurança da Informação

As etapas da segurança

- Mudanças dos padrões culturais – a política de segurança precisa ser construída desde o início, e não deve ser iniciada diretamente sobre as atividades de informática.
- "Vendendo a idéia" - consegue-se conscientizar mais facilmente as pessoas acerca da segurança se elas estiverem convencidas de que estão em primeiro lugar nas preocupações da política de segurança da organização. Tentar convencer o maior número possível de pessoas.
- A educação em segurança – Para convencer e obter apoio, antes de introduzir medidas de segurança, elabore um esquema de divulgação, na forma de palestras apresentações, cartazes nos quadros de avisos... Enfatize os aspectos positivos. Para isso conscientize a alta administração de que deve dar início à aplicação a política de segurança.

Aula 04

Segurança da Informação

As etapas da segurança

- Padronização – Um dos maiores aliados da segurança é a ordem.

A desorganização contribui decisivamente para o aumento não só da ineficiência como dos riscos relacionados com a segurança. Uma rotina desorganizada, sem documentação adequada, é uma fonte permanente de riscos e preocupações para a segurança.

A padronização facilita em alto grau o controle da execução da política de segurança em informática e ajuda a aumentar a produtividade e reduzir custos.

Uma nomenclatura-padrão que possa ser utilizada em toda a organização não precisa necessariamente começar pela área de informática, mas essa escolha é conveniente, se a empresa possuir uma área de informática centralizada.

Vantagens pessoais com relação a padronização: redução de trabalho desnecessário, melhoria de qualidade dos trabalhos apresentados, melhor conhecimento da estrutura de informações da organização...

Aula 04

Segurança da Informação

As etapas da segurança

• "Fechando o cerco"- Quando a cultura da organização tiver assimilado o padrão cultural da segurança como sua integrante, é chegada a hora da operacionalização da segurança dentro da estrutura administrativa da organização como um todo, e da estrutura de informática em particular.

• Operacionalização – O próximo passo após a organização ter assimilado e estar aplicando a segurança como parte de sua cultura, é montar a estrutura de controle e administração de segurança. Seguindo a etapas restantes (esta seqüência poderá ser alterada em função das conveniências de cada ambiente):

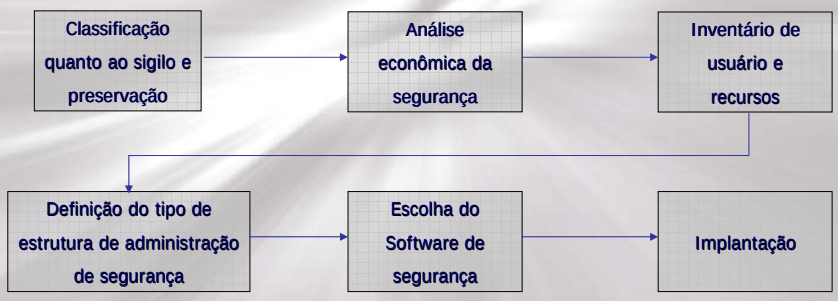
- Classificação quanto ao sigilo e preservação;
- Análise econômica da segurança;
- Inventário de usuários e recursos;
- Definição do tipo de estrutura de administração da segurança;
- Escolha das ferramentas de segurança;
- Implantação.

Aula 04

Segurança da Informação

Política de segurança

O modelo a seguir é uma sugestão. Cada organização está mais aparelhada para avaliar o modelo da política de segurança que melhor atenda a suas necessidades. Entretanto este modelo pode servir de base para qualquer organização que desejar usá-lo como roteiro de sua própria política de segurança.



* Seqüência das etapas de implantação da segurança

Aula 04

Segurança da Informação

Modelo de política de segurança

Objetivos

A política de segurança de informações de nossa organização visa atender aos seguintes objetivos:

1. Aparelhar a organização com um sistema capaz de assegurar a inviolabilidade dos ativos de informações.
2. Assegurar a segregação de funções.
3. Garantir a correta utilização do acervo de informações.
4. Garantir a correta utilização do ferramental de tratamento de informação.
5. Garantir a correta utilização do ferramental de segurança.

Aula 04

Segurança da Informação

Modelo de política de segurança

Abrangência

Todas as estruturas organizacionais que se utilizem de recursos de informações são obrigadas a seguir as diretrizes gerais desta política, como forma de gerenciar suas atividades.

Conceitos

Aplicam os conceitos a seguir no que se refere à política de segurança:

1. Política de segurança – conjunto de diretrizes destinadas a regulamentar o uso dos ativos de informações da organização.
2. Ferramentas - conjunto de equipamentos, programas, procedimento e demais recursos através dos quais se aplica a política de segurança.

Aula 04

Segurança da Informação

Conceitos

3. Propriedade de ativos - os ativos de informações da organização pertencem à mesma.

4. Acesso a ativos - a organização permite o acesso de terceiros a seus atira de informações para quem precisar fazer uso dos mesmos no desenvolvimento de suas atividades.

5. Direito de propriedade - dentro da organização, define-se como proprietário de um ativo o seu criador ou o principal usuário.

6. Custódia - define-se a custódia como a responsabilidade de se guardar um ativo para terceiros; entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros.

7. Direito de acesso - somente o proprietário do ativo, ou pessoa por ele nomeada, pode autorizar acesso ao mesmo.

Aula 04

Segurança da Informação

Conceitos

8. Validade do direito de acesso - somente é valido para os fins para os quais foi solicitado.

9. Direito de acesso em função da posição funcional - está ligado à posição ocupada pela pessoa dentro da organização, e não à pessoa que ocupa.

10. Controle de acesso - é exercido pela Administração de Segurança. As atribuições de controle de acesso podem ser delegadas para administradores setoriais e locais, para a administração de determinado domínio organizacional ou de recursos.

11. Proteção dos ativos - os ativos devem receber classificação quanto ao grau de sensibilidade para os negócios da organização. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que contém.

12. Responsabilidade - é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações.

Aula 04

Segurança da Informação

Responsabilidades dos funcionários

Todas os funcionários da organização são responsáveis pelas informações de que fazem uso e pelo respectivo ferramental de processamento de informações.

As responsabilidades são classificadas em função da posição hierárquica do funcionário dentro da organização.

Criptografia

Os funcionários devem usar criptografia, tanto para transmissão como para armazenamento de informações sensíveis.

Aula 04

Segurança da Informação

Chaves de acesso e senha

Os usuários deverão utilizar as informações por meio de chaves de acesso, autenticadas por senhas secretas de seu exclusivo conhecimento.

As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas. As operações realizadas sob o uso de determinada senha são de responsabilidade exclusiva de seu possuidor.

Aula 04

Segurança da Informação

Política de proteção de ativos

Alguns autores defendem a idéia de que as políticas devem resumir-se a umas poucas diretrizes que tenham a sua validade aceita por toda a corporação.

Modelo de política de proteção de ativos

A proteção de ativos, tais como máquinas, instalações, informações, bem como a integridade física dos funcionários são responsabilidade básica das gerências.

1. Pela identificação e proteção dos ativos sob sua guarda.
2. Por assegurar que todos os funcionários entendam as suas obrigações de proteger os ativos.
3. Pela implementação de procedimentos e práticas de segurança consistentes com a política de segurança.
4. Detecção de desvios com relação às práticas de segurança estabelecida e pela implementação da devida ação corretiva.

Segurança da Informação

Segurança da Informação

Termino da Aula 04