Curso de Tecnologia em Redes de Computadores
Disciplina: Auditoria e Análise de Segurança da Informação - 4º período
Professor: José Maurício S. Pinheiro

AULA 1 - Normas para Segurança Computacional

1. Uso das Normas

Normas são entendidas como um conjunto de regras ou orientações que visam qualidade, na atuação de uma tarefa. As normas em estudo buscam tornar o ambiente computacional das empresas mais seguro com relação a mitigar os incidentes computacionais, além de orientar sobre ações a serem tomadas, quando estes incidentes ocorrerem.

Aplicar normas de segurança em um ambiente computacional é mais do que modismo, é uma forma de garantir a existência de coerência nas ações dos coordenadores e executores das tarefas de administração dos ambientes computacionais. Adotar padrões reconhecidamente eficientes minimiza-se problemas de incidentes relacionados às operações sustentadas por computadores.

2. Tecnologia por si só não garante segurança da informação

Os dois itens mais importantes na hora de manter as informações da empresa em segurança são: a elaboração de políticas de segurança e o gerenciamento de suporte adequados, seguido do nível de conscientização dos funcionários.

A política de segurança atribui os direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham. Uma política de segurança também deve prever o que pode ser feito na rede da instituição e o que será considerado inaceitável. Tudo o que descumprir a política de segurança pode ser considerado um incidente de segurança.

Os incidentes de segurança devem ser notificados para os responsáveis pela máquina que originou a atividade e também para os grupos de resposta a incidentes e abusos das redes envolvidas. De modo geral a lista de pessoas/entidades a serem notificadas inclui os responsáveis pela rede que originou o incidente, incluindo o grupo de segurança e abusos, se existir um para aquela rede, bem como o grupo de segurança e abusos da rede em que o usuário está conectado, seja um provedor, empresa, universidade, etc.

3. *Entendendo a ABNT NBR ISO/IEC 27002*

Segurança para sistemas de informações foi um dos primeiros itens a definirem padrões. A gerência de segurança da informação visa identificar os riscos e implantar medidas que de forma efetiva tornem estes riscos gerenciáveis e minimizados.

A NBR ISO 27002 é um código de práticas de gestão de segurança da informação. Sua importância pode ser dimensionada pelo número crescente de pessoas e variedades de ameaças a que a informação é exposta na rede de computadores.

4. *Objetivos da norma*

O principal objetivo da Norma é estabelecer um referencial para as organizações desenvolverem, implementarem e avaliarem a gestão da segurança de informação. Em sua documentação a norma aborda 11 tópicos principais:

1. **Política de segurança** - onde descreve a importância e relaciona os principais assuntos que devem ser abordados numa política de segurança.
2. **Segurança organizacional** - aborda a estrutura de uma gerência para a segurança de informação, assim como aborda o estabelecimento de responsabilidades incluindo terceiros e fornecedores de serviços.
3. **Classificação e controle de ativos de informação** - trabalha a classificação, o registro e o controle dos ativos da organização.
4. **Segurança em pessoas** - tem como foco o risco decorrente de atos intencionais ou acidentais feitos por pessoas. Também é abordada a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e o treinamento em assuntos relacionados à segurança.
5. **Segurança ambiental e física** - aborda a necessidade de se definir áreas de circulação restrita e a necessidade de proteger equipamentos e a infra-estrutura de tecnologia de Informação.
6. **Gerenciamento das operações e comunicações** - aborda as principais áreas que devem ser objeto de especial atenção da segurança. Dentre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, homologação e implantação de sistemas, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda de backup, controle de documentação, segurança de correio eletrônico, entre outras.
7. **Controle de acesso** - aborda o controle de acesso a sistemas, a definição de competências, o sistema de monitoração de acesso e uso, a utilização de senhas, dentre outros assuntos.
8. **Desenvolvimento e manutenção de sistemas** - são abordados os requisitos de segurança dos sistemas, controles de criptografia, controle de arquivos e segurança do desenvolvimento e suporte de sistemas.

9. **Gestão de incidentes de segurança** - incluída na versão 2005, apresenta dois itens: Notificação de fragilidades e eventos de segurança da informação e gestão de incidentes de segurança da informação e melhorias.
10. **Gestão da continuidade do negócio** - reforça a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e atualizado.
11. **Conformidade** - aborda a necessidade de observar os requisitos legais, tais como a propriedade intelectual e a proteção das informações de clientes.

5. Norma ABNT NBR ISO/IEC-27001

A norma ABNT NBR ISO/IEC 27001:2005 relaciona os requisitos mandatários na definição do escopo do Sistema de Gestão da Segurança da Informação, a avaliação de riscos, a identificação de ativos e a eficácia dos controles implementados.

Esta Norma promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI - Sistema de Gerenciamento da Segurança da Informação, de uma organização. Para esta abordagem, a norma orienta à observação de um conjunto de ações e tarefas. Estas ações devem ser planejadas visando à eficiência de sua aplicação.

6. Entendendo a NBR 27001

A abordagem de processo para a gestão da segurança da informação apresentada nesta norma encoraja que seus usuários enfatizem a importância de:

- Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança da informação;
- Implantação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;
- Monitoração e analise crítica do desempenho e eficácia do SGSI;
- Melhoria contínua baseada em medições objetivas.

Administrar ambientes computacionais implica em atender as normas e diretrizes da organização. A não conformidade às normas ou o descumprimento ou a não observância implica em penalização legal por omissão a estas. A alegação de desconhecimento não tem valor legal.