

Segurança da Informação e Segurança em Redes de Computadores

Prof. Dr. Kelton Costa

kelton.costa@gmail.com

kelton.costa@unesp.br

Política de Segurança

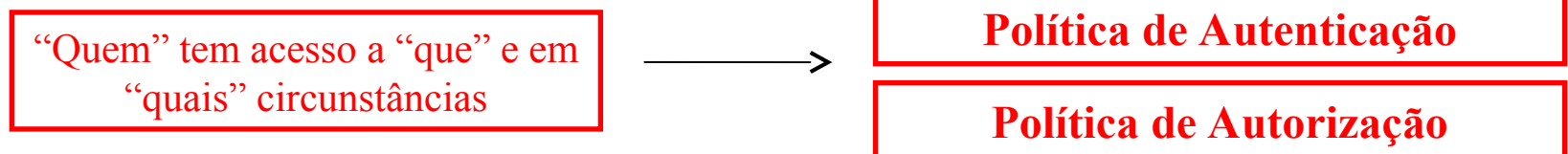
- O comprometimento com a segurança de sistemas deve surgir do mais alto nível da organização, alavancado pelo reconhecimento dos sérios problemas que poderiam resultar da divulgação, modificação ou indisponibilidade da informação.
- Esse comprometimento tende a ser expresso em uma política formal de segurança, estabelecida no contexto dos objetivos e funções organizacionais.
- Uma abordagem adotada por muitas organizações é a criação de uma política concisa e simples, que sirva de ponto de partida para outros documentos onde são estabelecidos os padrões, procedimentos e orientações para o comportamento dos usuários em relação à segurança.

Definição de Política de Segurança

- É o conjunto de regras e práticas que estabelecem os limites de operação dos usuários do sistema.
- Determina a maneira pela qual as informações e os recursos são administrados, protegidos e distribuídos no interior de um sistema específico.
- A política de segurança é feita sob medida para um sistema específico e não para uma classe geral de sistemas

Política de Segurança

- Possível dividir em:
 - **Física:** Se refere a situação física do sistema a proteger (incêndios e catástrofes naturais)
 - **Administrativa:** Ponto de vista organizacional no seio da empresa (seleção de pessoal responsável pela segurança)
 - **Lógica:** Define as regras de acesso e de circulação das informações no sistema (os controle para os acessos lógicos das informações)



Política de Autenticação

- **Autenticação:** um conjunto de procedimentos que permite que uma entidade (principal) comprove a sua identidade perante um sistema
 - Prova de identificação baseada em um segredo. Ex: Login (identificador) – Senha (password)
 - Dispositivo que possua. Ex: cartão magnético e smartcard
 - Traço pessoal (característica única). Ex: íris e impressão digital

Política de Autorização

- **Autorização:** é a função que decide se as requisições de acesso a objetos feitas por sujeitos devem ser ou não permitidas.

Exemplificando

O grupo SUPORTE é responsável pela manutenção e organização dos recursos computacionais, é encarregado de receber as críticas e sugestões dos usuários e de acatar as decisões da Comissão de Infraestrutura

Política Administrativa

Os Laboratórios de Informática devem possuir ar condicionado adequado para o bom estado de operação das máquinas e aterramento para todas os equipamentos da rede. As portas de acesso ao Lab X e ao Lab Y devem permanecer trancadas no horário do almoço (12:00-13:30) , das 18:00h até as 8:00h durante a semana e durante todo o final de semana

Política Física

Exemplificando

Os usuários deverão estar devidamente identificados com um crachá e com um *botom* para ter acesso aos laboratórios.

Restrições de acesso as impressoras:

- Epson: não há restrição
- HP Deskjet: grupo “Administração” não possui direito de acesso para imprimir
- HP LaserJet 1: os grupos “Computação” e “Funcionários” tem direito de acesso
- HP LaserJet 2: somente grupo “Professores” possui direito de acesso

Política Lógica

Como deve ser a Política de Segurança?

- Flexível;
- Simples;
- Objetiva;
- Regras Claras;
- Consistente;
- Aplicável;
- Viável;
- De acordo com as leis;
- Justificativa de cada norma;
- Responsabilidades;
- Consequências de não-cumprimento;
- Informações de contato;
- Privacidade;
- O que não consta;
- Continuidade (se aplicável)

Abrangência da Política de Segurança

- Não pode ser elaborada somente por uma pessoa (técnico);
- Tópicos:
 - Vigência (Início e Fim)
 - Importância da Política de Segurança;
 - Quais recursos são protegidos;
 - Quais aplicativos e softwares serão permitidos;
 - Qual procedimento para se conceder ou revogar privilégios na rede;
 - No caso de violação da política, o que deve ser feito?

Divulgação da Política de Segurança

- Avisos;
- Reuniões;
- Treinamentos Gerais e Departamentais ou Setoriais;
- Exemplificação através de informativos, jornais, peças teatrais e outros veículos de informação.

Se existe alguma política de segurança e as pessoas da organização não sabem, não serve para nada.

Processo de Implantação de uma Política de Segurança

1. Identificação dos recursos críticos
 - HW, SW, Dados, Pessoas, Documentação, Suprimentos
2. Classificação das Informações
 - Públicas, privadas, confidenciais, secretas
3. Definição, em linhas gerais, dos objetivos de segurança a serem atingidos
4. Análise das necessidades de segurança (identificação das ameaças, análise de riscos e impactos)

Processo de Implantação de uma Política de Segurança

5. Elaboração de proposta de política
6. Discussão aberta com os envolvidos
7. Apresentação de documento formal à gerência superior
8. Aprovação
9. Implementação e Treinamento
10. Avaliação da política e identificação das mudanças necessárias (constantemente)
11. Revisão

Responsabilidades com a Segurança

- Proprietário ou dono – responsável pelo negócio
- Gerente do Sistema – administração de recursos e infraestrutura/define a qualidade de serviço – Gerente de TI
- Usuário - ponta da estrutura de segurança de sistemas
 - deve obedecer as políticas de segurança
 - deve assinar um documento comprometendo-se a seguir as regras

Conscientização é uma medida de segurança poderosa

Segurança é uma atitude, uma filosofia a ser difundida por toda a instituição

O que fazer em Casos de Violação da Política de Segurança

- Ao detectar uma violação – determinar sua razão
 - Negligência, acidente ou erro, por desconhecimento da política ou ação deliberada ?
 - Circunstâncias da violação, como e porque ocorreu?
- Política – passos a serem seguidos para cada tipo de violação (ações corretivas e punição dos infratores)
- Treinamento do usuário – conscientização e divulgação da política de segurança

Roteiro para Auditoria da Política

- Foi elaborado, divulgado e é mantido atualizado o documento que descreve a política de segurança de informações ?
- A alta gerência está comprometida com a política por ela aprovada ?
- Foi definida uma estrutura organizacional responsável pela segurança ?
- Foram estabelecidos procedimentos de segurança de pessoal?
- Todos os funcionários conhecem os riscos de segurança e suas responsabilidades (treinamento)?
- São controlados e classificados os recursos computacionais?
- Foram definidos padrões adequados para segurança física?

Roteiro para Auditoria da Política

- Existe controle de acesso lógico aos sistemas ?
- Foram definidos procedimentos de backup e restauração de sistemas (foram testados) ?
- São investigados os incidentes de segurança ?
- Após uma violação da política, são tomadas as medidas necessárias para identificação de suas causas e agentes, são corrigidas as vulnerabilidades e os infratores são punidos ?
- Os aspectos de segurança são regularmente auditados a fim de verificar se as políticas estão sendo cumpridas ou se são necessárias modificações?

Gerência de Segurança

- Dependendo do tamanho da organização e do grau de vulnerabilidade dos dados devem existir **responsabilidade** pela segurança de informações – (pessoa ou grupo)
- Gerente responsável pela segurança
 - Auxiliar no desenvolvimento da política, divulgação e aplicação correta da política – ligação com alta gerência
 - Prevenir o acesso, impedir que danifiquem ou alterem qualquer coisa e saber recuperar os sistemas e dados (melhorar os controles para que o incidente não volte a acontecer)
- Mesmo que não haja o cargo alguém deve desempenhar essas funções