Política de Segurança da Informação

Política de Segurança

- Uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

- As políticas de segurança devem ter:
  - implementação realista
  - definição clara das áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção.
  - Deve também adaptar-se a alterações na organização.

Política de Segurança

- O documento que define a política de segurança:
  - Deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança
  - Deve ser também um documento de fácil leitura e compreensão, além de resumido.

- Existem duas filosofias por trás de qualquer política de segurança:
  - a proibitiva (tudo que não é expressamente permitido é proibido)
  - e a permissiva (tudo que não é proibido é permitido).

Garantias da Política de Segurança

- Os elementos da política de segurança deve garantir:
  - A Disponibilidade: o sistema deve estar disponível de forma que quando o usuário necessitar, possa usar. Dados críticos devem estar disponíveis ininterruptamente.
  - A Integridade: o sistema deve estar sempre íntegro e em condições de ser usado.
  - A Autenticidade: o sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.
  - A Confidencialidade: dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado

O que é Política de Segurança

- é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos.

- As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações.

Quem deve elaborar a PSI?

- É recomendável que na estrutura da organização exista uma área responsável pela segurança de informações, a qual deve iniciar o processo de elaboração da política de segurança de informações, bem como:
  - coordenar sua implantação, aprová-la e revisá-la
  - designar funções de segurança.

- Outros participantes:
  - áreas críticas da organização devem participar do processo de elaboração da PSI
  - a alta administração
  - os diversos gerentes e proprietários dos sistemas informatizados.

Quem deve aprovar a PSI?

- É recomendável que a PSI seja aprovada pelo mais alto dirigente da organização.

O que abordar na PSI?

- A política de segurança de informações deve extrapolar o escopo abrangido pelas áreas de sistemas de informação e pelos recursos computacionais:
  - Ela não deve ficar restrita à área de informática.
  - deve estar integrada à visão, à missão, ao negócio e às metas institucionais.

O que abordar na PSI?

- O conteúdo da PSI varia, de organização para organização:
  - em função de seu estágio de maturidade
  - grau de informatização
  - área de atuação
  - cultura organizacional
  - necessidades requeridas
  - requisitos de segurança
  - etc.

Tópicos comuns na PSI?

- definição de segurança de informações
- declaração do comprometimento da alta administração com a PSI, apoiando suas metas e princípios;
- objetivos de segurança da organização;
- definição de responsabilidades gerais na gestão de segurança de informações;
- orientações sobre análise e gerência de riscos;
- princípios de conformidade dos sistemas computacionais com a PSI;
- padrões mínimos de qualidade que esses sistemas devem possuir;
- políticas de controle de acesso a recursos e sistemas computacionais;
- classificação das informações (de uso irrestrito, interno, confidencial e secretas);

Tópicos comuns na PSI?

- procedimentos de prevenção e detecção de vírus;
- princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, direitos sobre software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);
- princípios de supervisão constante das tentativas de violação da segurança de informações;
- conseqüências de violações de normas estabelecidas na política de segurança;
- princípios de gestão da continuidade do negócio;
- plano de treinamento em segurança de informações.

Nível de detalhamento na PSI?

- Deve ser clara o suficiente para ser bem compreendida pelo leitor em foco, aplicável e de fácil aceitação.
  - A complexidade e extensão exageradas da PSI pode levar ao fracasso de sua implementação.

- quando a organização achar conveniente e necessário que sua PSI seja mais abrangente e detalhada, sugere-se a criação de outros documentos com regras mais específicas.

Nível de detalhamento na PSI?

- Cabe destacar que a PSI pode ser composta por várias políticas inter-relacionadas, como a política de senhas, de backup, de contratação e instalação de equipamentos e softwares.

Implantação da PSI?

- O processo de implantação da política de segurança de informações deve ser formal.
- passível a ajustes para melhor adaptar-se às reais necessidades.
- O tempo desde o início até a completa implantação tende a ser longo.
- As principais etapas que conduzem à implantação bem-sucedida da PSI são:
  - elaboração,
  - aprovação,
  - implementação,
  - divulgação e
  - Manutenção.

Implantação da PSI?

- De forma mais detalhada, pode-se citar como as principais fases que compõem o processo de implantação da PSI:
  - identificação dos recursos críticos;
  - classificação das informações;
  - definição, em linhas gerais, dos objetivos de segurança a serem atingidos;
  - análise das necessidades de segurança (identificação das possíveis ameaças, análise de riscos e impactos);
  - elaboração de proposta de política;
  - apresentação de documento formal à gerência superior;
  - aprovação

Implantação da PSI? (cont...)

- De forma mais detalhada, pode-se citar como as principais fases que compõem o processo de implantação da PSI:

  - publicação;
  - divulgação;
  - treinamento;
  - implementação;
  - avaliação e identificação das mudanças necessárias;
  - revisão.

O papel da alta administração

- O sucesso da PSI está diretamente relacionado com o envolvimento e a atuação da alta administração.

- Quanto maior for o comprometimento da gerência superior com os processos de elaboração e implantação da PSI, maior a probabilidade de ela ser efetiva e eficaz.

- O comprometimento deve ser expresso formalmente, por escrito.

A quem divulgar?

- Divulgação ampla a todos os usuários internos e externos à organização.

- É necessário que fique bastante claro, para todos, as consequências advindas do uso inadequado dos sistemas computacionais e de informações.

- É importante, ainda, que a PSI esteja permanentemente acessível a todos.

O que fazer quando houver violação?

- A própria Política de Segurança de Informações deve prever os procedimentos a serem adotados para cada caso de violação, de acordo com sua severidade, amplitude e tipo de infrator que a perpetra.

- A punição pode ser desde uma simples advertência verbal ou escrita até uma ação judicial.

O que fazer quando houver violação?

- A Lei n.º 9.983, de 14 de julho de 2000, que altera o Código Penal Brasileiro, já prevê penas para os casos de violação de integridade e quebra de sigilo de sistemas informatizados ou banco de dados da Administração Pública.

  - O novo art. 313-A, trata da inserção de dados falsos em sistemas de Informação

  - o art. 313-B discorre sobre a modificação ou alteração não autorizada desses mesmos sistemas.

  - O § 1º do art. 153 do Código Penal foi alterado e, atualmente, define penas quando da divulgação de informações sigilosas ou reservadas, contidas ou não nos bancos de dados da Administração Pública.

A Lei n.º 9.983

"Inserção de dados falsos em sistema de informações"

- "Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:"
  - "Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.“

"Modificação ou alteração não autorizada de sistema de informações“

- "Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:"
  - "Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa."
- "Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.”

O que fazer quando houver violação?

- O fornecimento ou empréstimo de senha que possibilite o acesso de pessoas não autorizadas a sistemas de informações é tratado no inciso I do § 1º do art. 325 do Código Penal.

- Neste tópico, fica ainda mais evidente a importância da conscientização dos funcionários quanto à PSI.

- Uma vez que a Política seja de conhecimento de todos da organização, não será admissível que as pessoas aleguem ignorância quanto às regras nela estabelecidas a fim de livrar-se da culpa sobre violações cometidas.

O que fazer quando houver violação?

- Quando detectada uma violação:
  - é preciso averiguar suas causas, consequências e circunstâncias em que ocorreu.
  - pode ter sido derivada de um simples acidente, erro ou mesmo desconhecimento da PSI
  - como também de negligência, ação deliberada e fraudulenta.
  - averiguação possibilita que vulnerabilidades, até então desconhecidas pelo pessoal da gerência de segurança, passem a ser consideradas, exigindo, se for o caso, alterações na PSI.

Conteúdo de uma Política

- Conteúdo básico de uma política:
  - Gerenciamento da Política de Segurança:
    - Definição da Segurança de Informações
    - Objetivo do Gerenciamento
    - Gerenciamento da Versão e Manutenção da Política
    - Referência para outras Políticas, Padrões e Procedimentos
  - Responsabilidades:
    - Definição das responsabilidades de segurança
    - Usuários de informações
    - Diretoria de Informática
    - Auditoria interna

Conteúdo de uma Política

- Conteúdo básico de uma política:
  - Classificação das informações
    - Introdução
    - Classificação
    - Manuseio da informação
    - Cuidados com impressora, copiadora e aparelhos de fax
    - Divulgação a terceiros
    - Propriedade intelectual
    - Privacidade da informação

Conteúdo de uma Política

- Conteúdo básico de uma política:
  - Procedimentos de segurança de informações
    - Gerenciamento de contas de acesso a sistemas e rede
    - Gerenciamento das senhas dos usuários
    - Controle de acesso ao S.O., B.D. e Sistemas aplicativos
    - Segurança física
    - Estações de trabalho
    - Manutenção e desenvolvimento de sistemas
    - Gerenciamento da segurança de rede
    - Acesso de terceiros
    - Monitoramento
    - Proteção contra *malwares*
    - Computadores móveis e acesso remoto
    - Uso de internet e correio eletrônico
    - Treinamento
    - Exceções da política de Segurança

Benefícios - Características

- Para que a política seja efetiva:
  - Ser verdadeira
    - Deve exprimir o pensamento da empresa
    - Coerente com as ações
    - Deve ser possível o seu cumprimento
  - Ser complementada com a disponibilização de recursos ($$$)
    - Liberação de $$$ e pessoal para implementação ao longo do tempo.
  - Ser válida para todos
    - A política deve ser cumprida por todos
    - Válida desde o Presidente até o estagiário
  - Ser simples
    - Fácil leitura e compreensão
    - Linguagem simples e direta
    - Evitar termos técnicos de difícil entendimento
  - Comprometimento da alta direção da organização
    - Documento assinado explicitando o seu total apoio à política

Benefícios – Curto prazo

- Formalização e documentação dos procedimentos de segurança adotado pela empresa
- Implementação de novos procedimentos e controles
- Prevenção de acessos não autorizados, falhas ou desastres
- Maior segurança nos processos de negócio

Benefícios – Médio prazo

- Padronização de procedimentos de segurança incorporados à rotina da empresa
- Adaptação segura de novos processos de negócio
- Qualificação e quantificação dos sistemas de resposta a incidentes
- Conformidade com padrões de segurança (ISO17799)

Benefícios – Longo prazo

- Retorno sobre o investimento
  - redução de incidência de problemas relacionados a segurança
  - Consolidação da imagem da empresa associada à segurança da informação

Penalidades

- Punições devem ser estabelecidas e aplicadas a todos pelo não cumprimento da Política de Segurança.
  - Definição de punições de acordo com a cultura da organização
  - Pode-se criar níveis de punições (máxima = demissão)
- O principal objetivo:
  - incentivar os usuários a aderirem à política
  - Respaldo jurídico à organização
- Qualquer violação deve ter conhecimento da alta administração
  - Escritório de segurança deve assegurar que o problema da violação foi resolvido e executada ações necessárias para evitar reincidências.

Prejuízos da ausência de Segurança

- Falha de segurança (estimativa para grandes empresas):
  - US$ 100 mil e 68 dias de trabalhos perdidos
- Fatores para aumento de falhas:
  - Falta de experiência
  - Má qualificação dos profissionais responsáveis pela segurança de dados
- Interrupção nas atividades informatizadas:
  - Parada nos negócios
    - Prejuízo financeiros
    - credibilidade junto ao mercado e clientes afetada
  - Dificuldades na recomposição das atividades
    - Falta de procedimentos adequados
    - Agravamento do item acima

Prejuízos da ausência de Segurança

- Maiores riscos na ausência de adequado nível de segurança:
  - Imagem e credibilidade poderão ser afetadas
  - Aumento de despesas com prejuízos por paralisação do negócio e vazamento de informações
  - Perdas por fraudes e erros
  - Novas aplicações e negócios comprometidos
  - Plano de continuidade inexistente (impossibilidade de continuar o processamento)
  - Concessão de acesso sem conhecimento do responsável
  - Ausência de procedimentos de backup, recuperação e armazenamento
  - Inexistência de monitoramento sobre cadastro de usuários
  - Divulgação de informações confidenciais.