Auditoria de Sistemas

Prof. Dr. Joseffe Barroso de Oliveira

AULA 06

Componentes de uma Política de Segurança

Introdução

Uma Política de Segurança é um conjunto de diretrizes e práticas estabelecidas para proteger os ativos de informação de uma organização. Seus componentes essenciais incluem o controle de acesso, que define quem pode acessar sistemas e dados; a gestão de incidentes de segurança, para lidar com ameaças e violações; e as regras de uso aceitável, que estabelecem limites para o uso de recursos de TI.

Fundamentos da Segurança da Informação

Confidencialidade

A confidencialidade é a garantia de que uma informação é acessível apenas às pessoas previamente autorizadas. A quebra de confidencialidade pode ocasionar danos inestimáveis para a empresa e seus clientes.

Integridade

A integridade envolve manter os dados intocados e preservados, garantindo que não sejam modificados ou eliminados sem autorização. A ruptura na integridade pode gerar impactos negativos significativos para uma empresa, especialmente em dados de alto valor.

Disponibilidade

A disponibilidade assegura que os colaboradores possam acessar os dados sempre que necessário, fundamental para operações como fechamento de contratos e vendas. A falta de disponibilidade pode resultar em prejuízos financeiros e de imagem.

Elaboração de uma Política de Segurança

- Definir os contornos e ferramentas necessárias, envolvendo todos os setores da organização para garantir que a política atenda aos requisitos específicos da empresa.
- Classificar as informações entre públicas, internas, confidenciais e secretos, para estabelecer níveis de acesso adequados a cada colaborador.
- Incluir a participação de diferentes equipes na definição de processos e tarefas que garantam a segurança, como cronogramas de backup e controle de acesso.
- A elaboração deve ser um esforço conjunto que garanta que 'todas as medidas, de alguma forma, impactam o trabalho de diferentes setores da empresa'.

Etapas de Implantação da PSI

Planejamento

Deve ser feito um planejamento que inclua o objetivo máximo da política, determine responsáveis e prazos, analisando o que deve ser protegido.

Documento de planejamento
Definição de responsáveis
Cronograma de implantação

Elaboração de Normas

Criação das normas relativas ao uso de programas, internet, dispositivos móveis, acesso à rede, bloqueio de sites e uso do e-mail corporativo.

Normas de uso
Documentação de proibições
Diretrizes de acesso

Aprovação pelo RH

O RH deve ler e aprovar o documento, conforme as leis trabalhistas e o manual interno dos empregados da organização.

Documento aprovado pelo RH
Relatório de conformidade
Comunicação aos colaboradores

Treinamento dos Colaboradores

Implantar a política comunicando todos os funcionários, que devem receber uma cópia do documento e treinamento prático sobre seus pontos principais.

Treinamento realizado
Declaração de comprometimento
Cópias da política distribuídas

Importância da Avaliação Contínua

- A avaliação contínua da política de segurança da informação é crucial para garantir sua eficácia.
- A política deve ser revisada regularmente, a fim de atualizá-la, caso seja necessário.
- A segurança da informação, por ter uma íntima relação com a tecnologia, está em constante evolução.
- Por esse e outros motivos, é imperioso manter uma rotina de avaliação, comparando os recursos de proteção internos da empresa à sofisticação das ameaças e, caso necessário, compatibilizando-os para que sejam suficientes e eficientes no combate às vulnerabilidades.