



ÍNDICE

POLÍTICA DE SEGURANÇA.....	2
PRINCÍPIOS DA POLÍTICA DE SEGURANÇA.....	2
CONFIDENCIALIDADE.....	2
INTEGRIDADE.....	2
DISPONIBILIDADE.....	2
AUTENTICIDADE.....	2
LEGALIDADE.....	2
CONFIABILIDADE.....	2
TOLERÂNCIA A FALHAS.....	2
NÃO-REPÚDIO.....	2
PRINCIPAIS AMEAÇAS À POLÍTICA DE SEGURANÇA.....	2
CONTROLES NECESSÁRIOS QUE DEVEM SER IMPLEMENTADOS NA POLÍTICA DE SEGURANÇA.....	2

WWW.LEITEJUNIOR.COM.BR
LEITEJUNIORBR@YAHOO.COM.BR

POLÍTICA DE SEGURANÇA

- A Tecnologia da informação só se torna uma ferramenta capaz de alavancar verdadeiramente os negócios, quando seu uso está vinculado à medidas de proteção dos dados Corporativos.
- É nesse contexto que a definição de um Modelo de Segurança da Informação deixa de ser custo associado a idéias exóticas, para se tornar investimento capaz de assegurar a sobrevivência da Empresa e a continuidade dos negócios da Organização.
- Para que as Empresas possam ser competitivas, é imperativo que elas possam contar com um trabalho de profissionais especializados e qualificados que saibam como alinhar Segurança à Tecnologia da Informação.

PRINCÍPIOS DA POLÍTICA DE SEGURANÇA

A Política de Segurança deve seguir alguns paradigmas básicos em sua composição.

CONFIDENCIALIDADE

- É a garantia do resguardo das informações dadas pessoalmente em confiança e a proteção contra a sua revelação não autorizada.
- Atualmente, confidencialidade é considerada como sendo o dever de resguardar todas as informações que dizem respeito a uma pessoa, isto é, a sua privacidade. A confidencialidade é o dever que inclui a preservação das informações privadas e íntimas.

INTEGRIDADE

- Condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas.

DISPONIBILIDADE

- É um sistema informático resistente a falhas de software e energia, cujo objetivo é manter os serviços disponibilizados o máximo de tempo possível.

AUTENTICIDADE

- É a certeza absoluta de que uma informação provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo.

LEGALIDADE

- Estado legal da informação, em conformidade com os preceitos da legislação em vigor.

CONFIABILIDADE

- Garantir que um sistema funcionará de forma eficiente e eficaz, de acordo com suas atribuições e funcionalidade.

TOLERÂNCIA A FALHAS

- Aumentar a confiabilidade de um certo sistema evitando falhas.
- Aumentar a disponibilidade do sistema, fazendo com que o sistema fique disponível por mais tempo.
- Estratégias de tolerância a falhas aumentam a confiabilidade e disponibilidade de sistemas.

NÃO-REPÚDIO

- Ou NÃO RECUSA é a garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação não negue, posteriormente, sua autoria.

PRINCIPAIS AMEAÇAS À POLÍTICA DE SEGURANÇA

- Falta de Integridade.
- Ameaças de Ambiente (fogo, enchente, tempestade ...).
- Erros humanos.
- Fraudes e erro de processamento.
- Indisponibilidade dos Sistemas.
- Divulgação da Informação premeditada e acidental.

CONTROLES NECESSÁRIOS QUE DEVEM SER IMPLEMENTADOS NA POLÍTICA DE SEGURANÇA

- Software de detecção de vírus e cavalos de tróia.
- Software de controle de acesso lógico.
- Mecanismos de controle de acesso físico.