



Introdução à Segurança da Informação

Everson Santos Araujo
everson@por.com.br

Segurança da Informação

Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaça a seu desenvolvimento

Conceituação segundo o DOU de 14/06/2000

Necessidade da Segurança



* Reduzir os riscos

- Fraudes
- Acesso indevido
- Uso indevido
- Sabotagens
- Roubo
- Erros

Medidas para garantir segurança



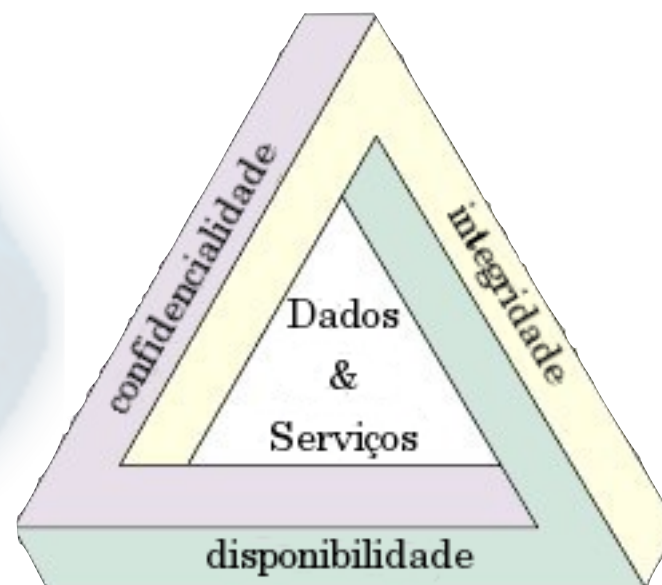
* Proteger

- O que?
- De quem?
- A que custos?
- Com que riscos?

Princípios

* A Segurança da Informação deve seguir três princípios básicos:

- Confidencialidade
- Integridade
- Disponibilidade



Confidencialidade



- * É a garantia do resguardo das informações dadas pessoalmente em confiança e a proteção contra a sua revelação não autorizada

Glossário de Bioética do Instituto Kennedy de Ética

- * Criptografia é a arte e ciência de guardar e transmitir dados confidenciais

Criptografia

- * Criptografia, do grego **kryptos** (*escondido, oculto*) mais a palavra **grápho** (*grafia, escrita*), é a ciência de escrever em códigos ou em cifras, ou seja, através de uma série de procedimentos transforma-se um texto "em claro" (*inteligível*) em um texto "cifrado" (*ininteligível*)

Integridade



- * Dados não podem ser criados, alterados, ou removidos sem autorização
- * É a garantia de que a informação não foi alterada durante a sua transmissão.
- * Tipos de integridade
 - Receptor – Assinatura digital
 - Dados – Algoritmos de hash

Algoritmo hash

- * Função que recebe uma quantidade arbitrária de dados e os comprime retornando um número fixo de bits



Assinatura Digital



- * Baseado em criptografia assimétrica
- * Utilizando chaves públicas e privadas
- * Funcionamento
 - Gera um resumo da mensagem
 - *message digest*
 - Criptografa esse resumo com sua chave privada, garantindo assim a autenticidade e o não-repúdio

Disponibilidade



- * Necessidade de um serviço estar disponível para os usuários sempre que eles necessitarem das informações
- * Protocolos de alta disponibilidade

Alta Disponibilidade



- * Sistema alternativo que entra em funcionamento logo que o sistema, ou parte do sistema, principal falha