Segurança da Informação

Princípios Básicos

Igor Machado Coelho

20/03/2024

Section 1

Módulo: Princípios Básicos

Pré-Requisitos

São requisitos para essa aula o conhecimento de:

- Redes de Computadores (conceitos gerais)

Tópicos

- Histórico
- Conceitos
- Desafios
- Princípios Básicos
- Ciclo de Vida da Informação

Section 2

Princípios Básicos

Histórico

- Nasceu como elemento de estratégia militar
  - Assim como a ARPANET, ...
- Amadureceu em entidades militares, governamentais e Acadêmicas
- Desde a década passada faz parte da estratégia corporativa

Conceitos

O que é a Informação?

"Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos ou transacionais"
(Marcos Sêmola)

O que é a Segurança?

"[...] um estado e qualidade ou condição de seguro, assim também como convicção e certeza"
(Dicionário Aurélio)

DEFINIÇÕES DE SEGURANÇA DA INFORMAÇÃO

- Segurança da Informação é a proteção da **informação** de vários tipos de **ameaças** para a **continuidade do negócio** e também para **minimizar o risco** ao negócio.
- Segurança da Informação: área do conhecimento dedicada à **proteção de ativos da informação** *contra* **acessos não autorizados, alterações indevidas** ou a sua **indisponibilidade**.

Dados vs Informação

O termo Segurança da Informação aborda, de forma equivalente, o que é compreendido como dado ou como informação.

SEGURANÇA COMPUTACIONAL

- Proteção oferecida a um sistema de informação automatizado para atingir os objetivos aplicáveis de preservar a integridade, disponibilidade e confidencialidade dos recursos do sistema de informação
- Inclui hardware, software, firmware, informações / dados e telecomunicações

Indo além das redes

O termo Segurança da Informação pode ser expandido para diversas outras áreas da computação, incluindo não apenas software.

DESAFIOS GERAIS

- Definição das Funções e Responsabilidades;
- Participação ativa nas estratégias organizacionais;
- Integração com a missão da Organização.

DESAFIOS ESPECÍFICOS

1. Não é simples
2. Deve considerar possíveis ataques
3. Usa procedimentos não intuitivos
4. Envolve algoritmos e informações secretas
5. Deve decidir onde implantar mecanismos
6. Batalha de inteligência entre atacante/administrador
7. Benefício não percebido até falhar
8. Requer monitoramento regular
9. Muitas vezes um pensamento posterior
10. Considerado impedimento ao uso do sistema

CONCEITOS CHAVE

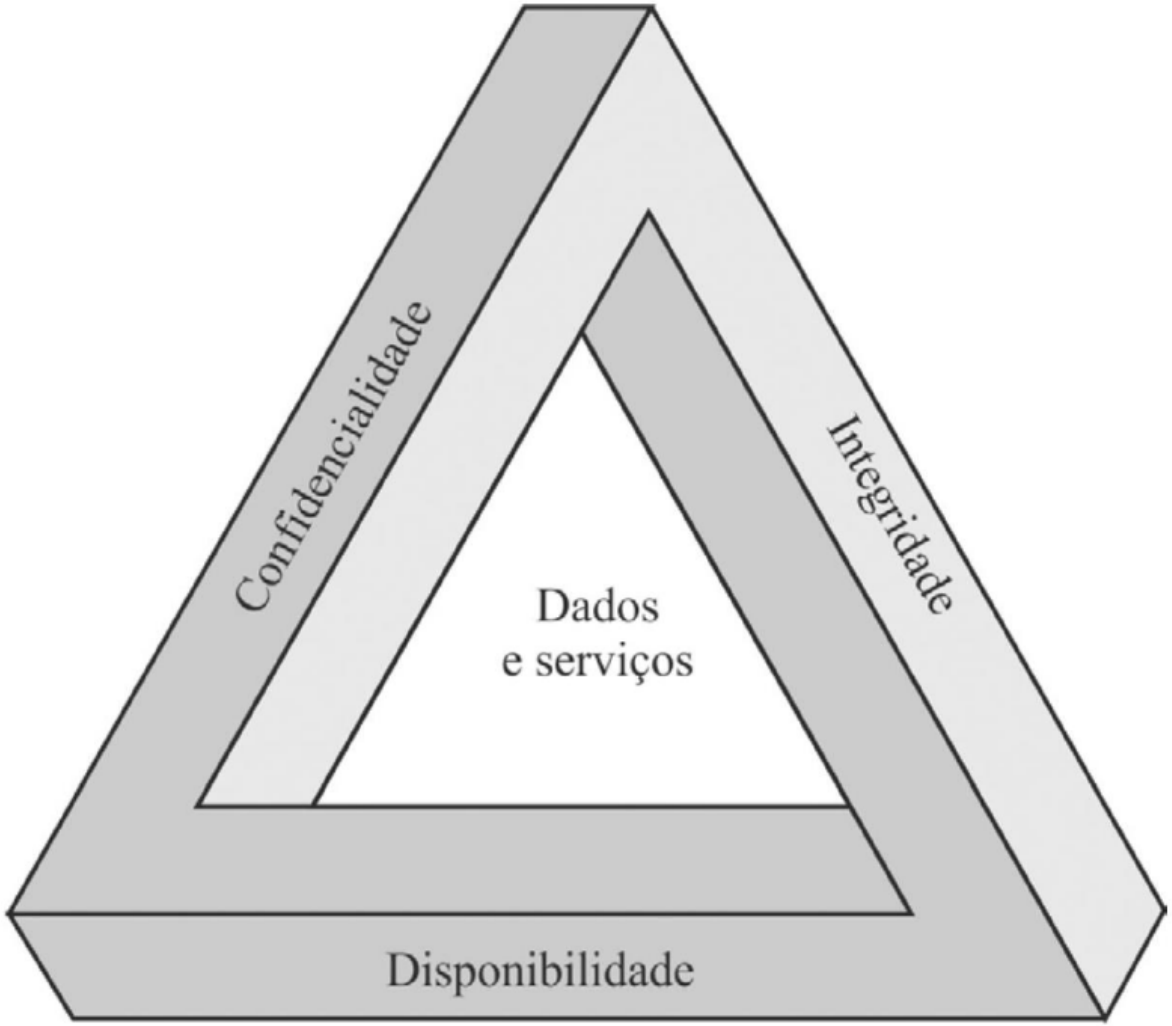

Figure 1: fonte: Segurança de Computadores de W. STALLINGS

PRINCÍPIOS BÁSICOS

CONFIDENCIALIDADE

Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas

INTEGRIDADE

Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais. Garantir que as informações sejam alteradas somente pelas pessoas que possuem acesso para tal!

DISPONIBILIDADE

Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade

ASPECTOS DE SI / CONCEITOS ADICIONAIS

Alguns aspectos são complementares à tríade CID, sendo Autenticação considerado por alguns[1] como parte da Integridade.

AUTENTICIDADE

Garantia de que as entidades (informação, máquinas, usuários) identificadas em um processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após seu envio ou validação

LEGALIDADE / Determinação de Responsabilidade

Caraterística das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes

[1] FIPS PUB 199

CICLO DE VIDA DA INFORMAÇÃO (Parte 1/2)

É fundamental ter atenção a todas as quatro etapas do ciclo de vida da informação: manuseio; armazenamento; transporte e descarte.

MANUSEIO

Momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação Internet, ou ainda, ao utilizar sua senha de acesso para autenticação, por exemplo.

ARMAZENAMENTO

Momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou ainda, em uma mídia de disquete/pendrive depositado na gaveta da mesa de trabalho, por exemplo

CICLO DE VIDA DA INFORMAÇÃO (Parte 2/2)

TRANSPORTE

Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico (email), ao postar um documento via aparelho de fax, ou ainda, ao falar ao telefone uma informação confidencial, por exemplo

DESCARTE

Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um CD/DVD usado que apresentou falha na leitura

Section 3

Discussão

Breve discussão

Cenário atual: instituições públicas e privadas da região

- Será que as instituições da região tem cumprido com a responsabilidade de segurança debatida até o momento?
- Como as equipes podem ser melhor treinadas e aprimoradas para esse cumprimento?
- Recomendada leitura de material complementar (material acessível a executivos e público-geral): "SÊMOLA, Marcos. Gestão da Segurança da Informação, 2a Ed. Elsevier Brasil, 2014."

Leia mais (parte 1/2)

Os **conceitos básicos** estão apresentados no documento:

- NIST FIPS PUB 199 (fev./2004)
  - Standards for Security Categorization of Federal Information and Information Systems
  - 13 páginas
  - https://csrc.nist.gov/pubs/fips/199/final

Mais referências, procurar no Handbook do NIST:

- NIST Special Publication 800-12
  - An Introduction to Information Security (out./1995)
  - 101 páginas
  - https://doi.org/10.6028/NIST.SP.800-12r1
  - https://www.nist.gov/publications/introduction-computer-security-nist-handbook
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Leia mais (parte 2/2)

Livro:

- "Segurança de Computadores - Princípios e Práticas - 2012" - Stallings, William; Brown, Lawrie & Lawrie Brown & Mick Bauer & Michael Howard
  - Em Português do Brasil, CAMPUS - GRUPO ELSEVIER, 2ª Ed. 2014

Veja Capítulo 1, "Seção 1.1 - Conceitos de Segurança de Computadores".

Section 4

Agradecimentos

Pessoas

Em especial, agradeço aos colegas que elaboraram bons materiais, como o prof. Raphael Machado, Kowada e Viterbo cujos conceitos formam o cerne desses slides.

Estendo os agradecimentos aos demais colegas que colaboraram com a elaboração do material do curso de Pesquisa Operacional, que abriu caminho para verificação prática dessa tecnologia de slides.

Software

Esse material de curso só é possível graças aos inúmeros projetos de código-aberto que são necessários a ele, incluindo:

- pandoc
- LaTeX
- GNU/Linux
- git
- markdown-preview-enhanced (github)
- visual studio code
- atom
- revealjs
- groomit-mpx (screen drawing tool)
- xournal (screen drawing tool)
- ...

Empresas

Agradecimento especial a empresas que suportam projetos livres envolvidos nesse curso:

- github
- gitlab
- microsoft
- google
- ...

Reprodução do material

Esses slides foram escritos utilizando pandoc, segundo o tutorial ilectures:

- https://igormcoelho.github.io/ilectures-pandoc/

Exceto expressamente mencionado (com as devidas ressalvas ao material cedido por colegas), a licença será Creative Commons.

Igor Machado Coelho

This Slide Is Intentionally Blank (for goomit-mpx)