



## Aula 1

### Segurança em Sistemas de Informação

Prof. Me. Luis Gonzaga de Paulo

### Fundamentos de Segurança da Informação

## Agenda

- A informação
- Segurança da informação
- Proteção da Informação
- Vulnerabilidades e risco
- Gestão de riscos

## Contextualizando

- A Era da Informação
- A importância da informação
- Incidentes de Segurança
- Proteção e mitigação
- Uso indevido

## A Informação

- A quantidade
- O impulso da imprensa, fotografia e telégrafo

- Computador e internet
- O valor da informação
- Dados X informação



- Produzimos e utilizamos enormes quantidades de informação. Estima-se em 1.000 Terabytes ( $10^{15}$  bytes) a quantidade de dados médicos digitalizáveis de cada ser humano!

- E se consideramos:
  - e-mails
  - fotos
  - áudios
  - vídeos... ?

- A informação é tudo aquilo que podemos experimentar com os nossos sentidos. Tem propósito para seu uso. E tem um valor. Em TIC diferencia-se dado de informação

- O dado é:
  - elemento
  - valor
  - grandeza

- A informação tem um valor intrínseco que deve ser preservado. É um ativo, bem, patrimônio das pessoas e das organizações. Suas características:

- formas
- meios
- armazenamento
- transporte
- modificação



- 13/59
- O valor da informação é a base para a sua classificação: confidencial, secreta, reservada, pública. E a classificação define grau de sigilo e confidencialidade. (...)

14/59

(...) Ou seja, os mecanismos de controle e as proteções necessárias para preservar o valor da informação

- 15/59
- A informação possui um ciclo de vida:
    - criação
    - manuseio
    - armazenamento
    - transporte
    - descarte

## A Segurança da Informação

- 16/59
- Proteção da informação
  - Preservação do valor da informação

- 17/59
- Processos
  - Técnicas
  - Ferramentas
  - Mecanismos

- 18/59
- Segurança é um conceito bastante amplo, ligado à garantia, proteção e preservação. Em TI, a segurança pode referir-se a três aspectos distintos:



- **security**
- **reliability**
- **safety**

• **Todos relacionados à Segurança da Informação**

19/59

• **A segurança da informação pretende preservar o valor da informação, protegendo-a. Essa proteção é resultado de um conjunto de controles que incluem:**

20/59

- **políticas**
- **processos**
- **estrutura**
- **software**
- **hardware**

21/59

• **A segurança da informação contempla três características fundamentais – aspectos básicos – da informação, para as quais busca-se a preservação, a saber:**

22/59

- **confidencialidade**
- **integridade**
- **disponibilidade**

23/59

• **Além destas três características fundamentais, outros aspectos decorrente do uso da Tecnologia da Informação e das Comunicações são considerados:**

24/59



- autenticidade
- irretratabilidade
- legalidade
- privacidade
- auditabilidade

25/59

- A segurança da informação é suportada e propiciada pelas atividades de três áreas distintas e interdependentes entre si, a saber:

26/59

- segurança física
- segurança da infraestrutura
- segurança do software, lógica ou de sistemas

27/59

## A Proteção da Informação

- Níveis: estratégico, tático e operacional
- Métodos
- Processos
- Técnicas
- Ferramentas
- Mecanismos

28/59

- Princípio básico da segurança: a organização estará segura somente se todos estiverem seguros, seguindo a Política de Segurança da Informação, que deve pautar-se por:

29/59

- objetivos claros
- tolerância ao risco
- orientação para as iniciativas
- comprometimento

30/59



- A política de segurança da informação não é algo abstrato, inexecutável, perfeito e acabado. Deve ser coerente com o negócio e estar de acordo com:

- legislação
- normas
- regulamentos
- governança, ou seja, *compliance*

- A Política de Segurança da Informação regula e dissemina as práticas necessárias para atingir o nível de segurança desejado, por meio de:

- hierarquia e responsabilidades
- abrangência: pessoas, processos e tecnologia
- objetivos mensuráveis
- evolução constante

## Vulnerabilidades e Risco

- A informação no processo produtivo
- Os ativos
- Vulnerabilidades
- Ameaças
- Risco

- A informação é útil à medida em que é integrada ao processo produtivo, resultando na interação decorrente de seu ciclo de vida, ou seja, manuseio e exposição à:



- uso intensivo
- novas tecnologias
- interesses diversos
- falhas, ou seja, pontos fracos ou vulnerabilidades

- Para interagir com a informação e utilizá-la adequadamente no processo produtivo é necessário prover meios – os ativos – típicos das TICs, tais como:

- dispositivos
  - componentes
  - circuitos
  - programas...
- Além dos processos e das pessoas

- Os agentes ou eventos – ameaças – podem explorar ou interagir com as vulnerabilidades desses ativos, os incidentes de segurança. O risco é a probabilidade que isso ocorra



- A análise de riscos usa o histórico, a estatística e a probabilidade para avaliar a exposição ao risco e o impacto de sua ocorrência, considerando:



- ativos
- vulnerabilidades
- controles
- ameaças
- probabilidade
- impacto

43/59

## Gestão de Risco

- Os processos
- *Asset assessment*
- Análise quantitativa
- Análise qualitativa
- ROI
- Tratamento dos riscos

44/59

- A gestão de riscos é a atividade voltada para conhecer e tratar adequadamente os riscos e garantir o nível adequado de segurança da informação, usando os seguintes processos:

45/59

- identificação de ativos
- análise de riscos
- planejamento e abordagem
- monitoramento e controle

46/59

- A identificação dos ativos, *asset assessment*, o valor e também as vulnerabilidades vinculadas a estes mesmos ativos é o primeiro passo para evitar os incidentes, provendo:

47/59

- identificação
- descrição
- localização e uso
- controles existentes
- exposição a ameaças

48/59





- A análise quantitativa dos riscos avalia a probabilidade e o impacto dos riscos, por meio de criação de uma Matriz PxI, classificação e priorização do tratamento dos riscos

|               |   |         |    |    |    |    |
|---------------|---|---------|----|----|----|----|
| Probabilidade | 5 | 5       | 10 | 15 | 20 | 25 |
|               | 4 | 4       | 8  | 12 | 16 | 20 |
|               | 3 | 3       | 6  | 9  | 12 | 15 |
|               | 2 | 2       | 4  | 6  | 8  | 10 |
|               | 1 | 1       | 2  | 3  | 4  | 5  |
|               |   | Impacto |    |    |    |    |
|               |   | 1       | 2  | 3  | 4  | 5  |

Legenda  
 ■ Alto  
 ■ Médio  
 ■ Baixo

- A análise qualitativa dos riscos usa o valor financeiro ligado ao risco – perdas de vendas ou de reputação, multas, custo da oportunidade ou de reposição – para definir o tratamento e o ROI:

- valor do ativo
- expectativa de perdas
- custo do tratamento
- ROI

- O tratamento do risco decorre das estratégias estabelecidas para a definição e aplicação de controles, mecanismos de proteção e defesa. Trata-se de optar por:

- reduzir
- reter ou evitar
- transferir
- aceitar o risco



## Síntese

- Informação
- Segurança da Informação
- Proteção da informação
- Vulnerabilidades e riscos
- Gestão de riscos

55

59

## Referências de Apoio

- GALVÃO, M. da C. Fundamentos em Segurança da Informação. São Paulo: Pearson Education, 2015.

56

59

- ISO 27002:2013. Segurança da Informação: coletânea eletrônica, Rio de Janeiro: ABNT, 2014.

57

59

- PAULO, W. L. de; FERNANDES, F. C.; RODRIGUES, L. G. B.; EIDIT, J. Riscos e controles internos: uma metodologia de mensuração dos níveis de controle de riscos empresariais. *In: Revista Contabilidade e Finanças*, v. 18. n. 43. USP, São Paulo, jan/abr. 2007.

58

59

- PMI, A Guide to the Project Management Body of Knowledge (PMBOK GUIDE). Project Management Institute, 2013.

59

59



60

59