

Agenda

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

Contextualizando

- A Era da Informação
- A importância da informação
- J 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

Núcleo de Materiais Didáticos

■ Produzimos e
utilizamos enormes
quantidades de
informação.
Estima-se em
1.000 Terabytes
(10¹⁵ bytes) a
quantidade de
dados médicos
digitalizáveis de
cada ser humano!

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:

o formas o meios o armazenamento o transporte o modificação O valor da informação é a base para a sua classificação: confidencial, secreta, reservada, pública. E a classificação define grau de sigilo e confidencialidade.

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

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

A Segurança da Informação

- Proteção da informação
- Preservação do valor da informação

- Processos
- Técnicas
- Ferramentas
- Mecanismos

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

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

- políticas
- processos
- estrutura
- software
 - hardware

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

- confidencialidade
- integridade
- disponibilidade

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

- autenticidade
- irretratabilidade
- legalidade
- privacidade
- auditabilidade

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

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

A Proteção da Informação

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

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:

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

A política de segurança da informação não é algo abstrato, inexequível, 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

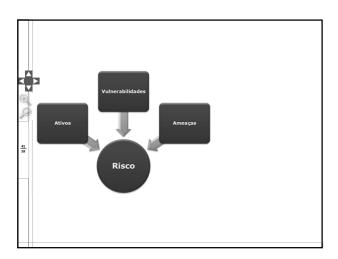
A informação é útil à medida em que é integrada ao processo produtivo, resultando na interação decorrente de seu ciclo de vida, ou seja, manuseio e exposição à:

- 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 dosprocessos edas 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

Gestão de Risco

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

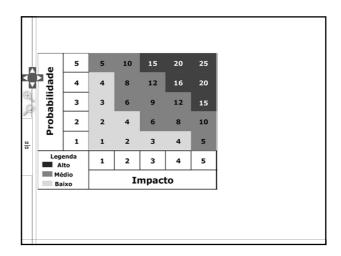
A gestão de riscos é a atividade voltada para conhecer e tratar adequadamente os riscos e garantir o nível adequado de segurança da informação, usando os seguintes processos:

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

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:

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

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



■ 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

Referências de Apoio

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

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

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.

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

