# PÓS EM COMÉRCIO EXTERIOR E ESTRATÉGIA

## UNIVERSIDADE CATÓLICA DE PETRÓPOLIS

## CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

# TECNOLOGIA DA INFORMAÇÃO

# .:UNIDADE 05 - SEGURANÇA DA INFORMAÇÃO:.

# PARTE 1 – INTRODUÇÃO E CONCEITOS

VERSÃO: SETEMBRO DE 2018

Professor: Luís Rodrigo de O. Gonçalves

E-mail: luis.goncalves@ucp.br
Site: http://lrodrigo.sgs.lncc.br

# (1) Segurança da Informação

# Segurança da Informação
## INTRODUÇÃO



- Relaciona-se com **proteção** de um conjunto de **informações**; **preservando** o seu **valor**.
- A **Informação** passa a ser vista como um **Ativo**.
- **Não** está restrita **apenas** aos sistemas **computacionais**

# Segurança da Informação
## INTRODUÇÃO



**Seg. Informática ou Seg. de Computadores**:

- Relaciona-se com o de Seg. da Informação;
- Envolve a segurança dos **dados/informação**
- E a segurança do **sistema**.

# Segurança da Informação
## INTRODUÇÃO



- A família de normas **ISO/IEC 27000** converge para o Sistema de Gestão de Segurança da Informação (**SGSI**);
- O SGSI é uma forma de segurança para **todos os tipos de dados e informações**
- As normas mais divulgadas as **27001** e **27002**.
- Antes da Serie 27000, havia a norma ISO/IEC **17799:2005**, influenciada pelo padrão inglês (British Standard) **BS 7799**.

# SEGURANÇA DA INFORMAÇÃO - CONCEITOS

# Segurança da Informação
## CONCEITOS



**Definições de Seg. da Info. mais importantes**:

- ✓ a **proteção** contra o **uso ou acesso** não-autorizado à informação
- ✓ proteção contra a **negação do serviço** a usuários autorizados
- ✓ preservação da **integridade** e a **confidencialidade** da informação

# Segurança da Informação

## CONCEITOS



- ✓ A Seg da Info. se aplica à todos os aspectos de proteção da **informação ou dados**, para **qualquer formato**.
- ✓ O **nível de proteção** deve corresponder ao **valor** da **informação** e aos **prejuízos** que podem decorrer do seu uso impróprio.
- ✓ Seg. da Info. deve **cobrir** toda a **infraestrutura** que permite o seu uso, como **processos**, **sistemas**, **serviços**, **tecnologias**, e outros.

# Segurança da Informação
## CONCEITOS



- ✓ A **Informação** pode estar guardada para uso **restrito** ou exposta ao **público** para consulta ou aquisição.
- ✓ Devem ser estabelecidas **métricas** para a definição do **nível de segurança** e métodos para **verificação**
- ✓ A seg. pode ser afetada por: (i) fatores comportamentais, (ii) pelo ambiente, (iii) pela infraestrutura e/ou por (iv) pessoas mal intencionadas com objetivo de furtar, destruir ou modificar tal informação.

# Segurança da Informação
## CONCEITOS



- A tríade **CIA (Confidentiality, Integrity and Availability)** — Confidencialidade, Integridade e Disponibilidade — representa os principais atributos que orientam:
  - a análise,
  - o planejamento
  - a implementação da segurança

# Segurança da Informação
## CONCEITOS



Outros atributos das informações:

- ✓ Não-repúdio (irretratabilidade),
- ✓ Autenticidade
- ✓ Conformidade (legal).
- ✓ Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

# Segurança da Informação

## CONCEITOS



**Atributos básicos da Seg. da Inf. segundo a ISO/IEC**:

- ✓ **Confidencialidade**: limitar o acesso apenas às entidades legítimas - àquelas autorizadas pelo proprietário da informação;
- ✓ **Integridade**: garantir que a informação manipulada mantenha todas as características, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente).

# Segurança da Informação
## CONCEITOS



**Atributos básicos da Seg. da Inf. segundo a ISO/IEC:**

- ✓ **Disponibilidade**: garantir que a informação esteja sempre disponível, para o uso legítimo, ou seja, para os usuários autorizados;
- ✓ **Autenticidade**: garantir que a informação é proveniente da fonte anunciada e que não foi alvo de alterações ao longo de um processo;

# Segurança da Informação
## CONCEITOS



**Atributos básicos da Seg. da Inf. segundo a ISO/IEC:**

- ✓ **Irretratabilidade ou não repúdio**: garantir a impossibilidade de negar a autoria em relação a uma transação/operação/ação;
- ✓ **Conformidade**: garantir que o sistema segue as leis e regulamentos.

# MECANISMOS DE SEG. DA INFO.

# Segurança da Informação

## MECANISMOS DE SEGURANÇA



- **Controles físicos**: barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura.
- Mecanismos de segurança que apoiam os controles físicos:
  - portas, **trancas**, paredes, **blindagem**, guardas, etc.

# Segurança da Informação

## MECANISMOS DE SEGURANÇA



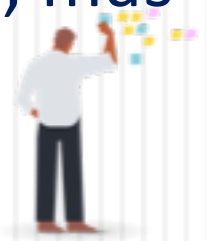
- **Controles lógicos**: barreiras que impedem ou limitam o acesso a informação
  - Localizado em ambiente controlado, geralmente eletrônico
  - Sem ele as informações ficariam expostas à alteração não autorizada.

# Segurança da Informação

## MECANISMOS DE SEGURANÇA



- **Controles lógicos**:
  - **Mecanismos de cifração ou encriptação e decifração**: permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros.
  - **Assinatura digital**: dados criptografados associados a um documento; garantem a **integridade** e **autenticidade** do documento, mas não a sua confidencialidade.



# Segurança da Informação

## MECANISMOS DE SEGURANÇA



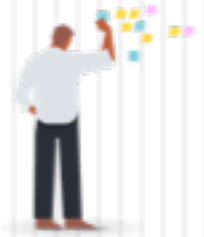
- **Controles lógicos**:
  - Mecanismos de **garantia da integridade da informação**: funções de "Hashing" ou de checagem; verifica/garante a integridade através de comparação do resultado obtido com o divulgado pelo autor.
  - Mecanismos de **controle de acesso**: palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.

# Segurança da Informação

## MECANISMOS DE SEGURANÇA



- **Controles lógicos**:
  - Mecanismos de **certificação**: atesta a validade de um documento.
  - **Honeypot**: tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor; É uma espécie de armadilha para invasores; mas não oferece nenhum tipo de proteção.

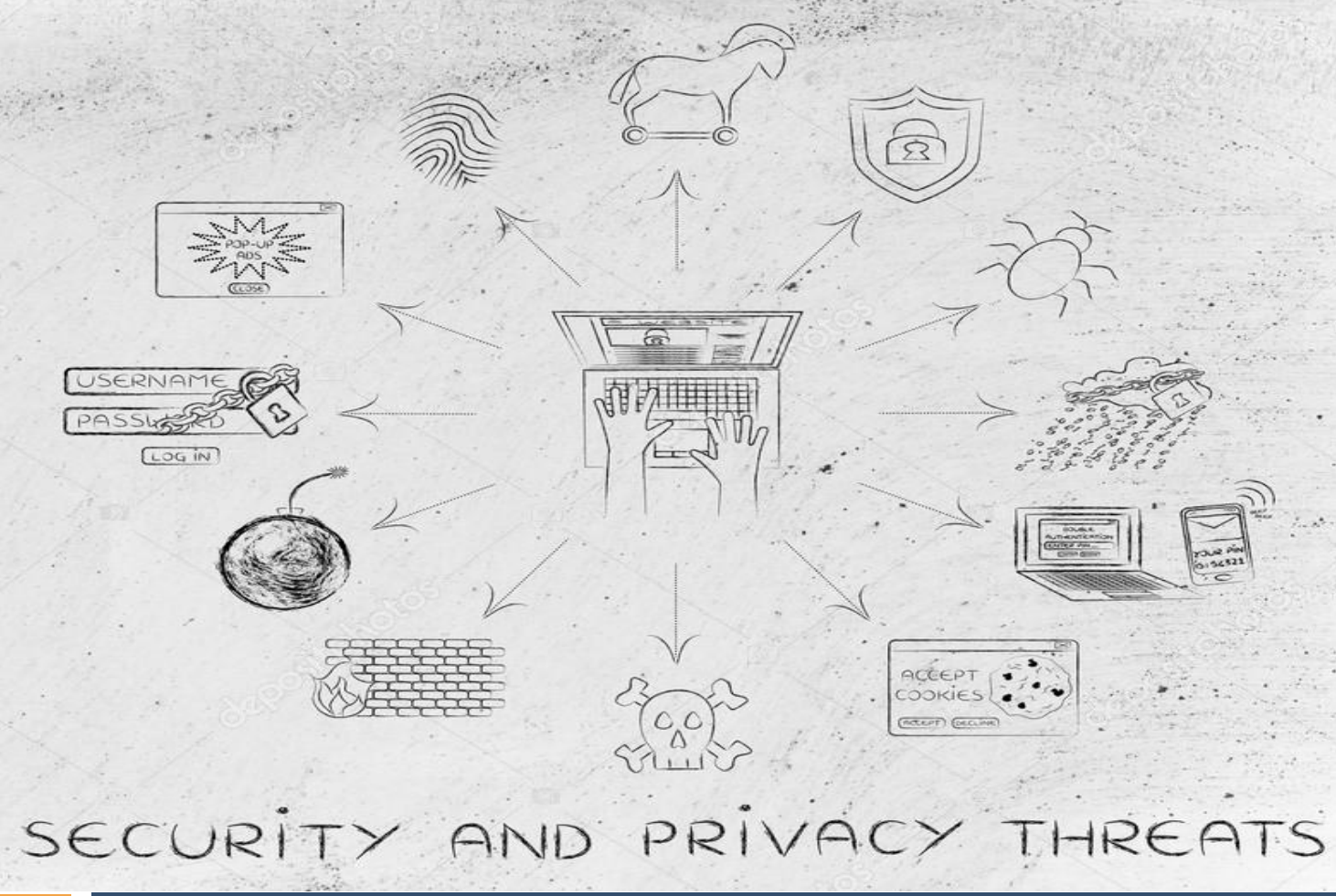


# Segurança da Informação

## MECANISMOS DE SEGURANÇA



- **Controles lógicos**:
  - **Protocolos seguros**: uso de protocolos que garantem um grau de segurança e usam alguns dos mecanismos citados aqui.
  - Atualmente existe uma grande variedade de **ferramentas e sistemas** que pretendem fornecer segurança. Alguns exemplos: antivírus, firewalls, filtros anti-spam, fuzzers, detectores de intrusões (IDS), analisadores de código.




# AMEAÇAS À SEGURANÇA

# Segurança da Informação

## AMEAÇAS À SEGURANÇA



**Relacionadas à perda de uma da seguintes características:**

- **Perda de confidencialidade**: há uma **quebra de sigilo** de uma determinada informação; informações restritas podem ser expostas;
- **Perda de integridade**: uma pessoa não autorizada efetua **alterações que não foram aprovadas** e não estão sob o controle do proprietário da informação;
- **Perda de disponibilidade**: a informação **deixa de estar acessível**. Perda de comunicação com um sistema importante; queda de um servidor ou de uma aplicação crítica, devido a uma ação não autorizada de pessoas com ou sem má intenção.

# Segurança da Informação

## AMEAÇAS À SEGURANÇA



**Ameaças podem vir de agentes maliciosos:**

- Muitas vezes conhecidos como crackers;
- Motivados por: notoriedade, autoestima, vingança e enriquecimento ilícito.
- Segundo o Computer Security Institute, mais de 70% dos ataques partem de usuários legítimos (insiders);
- Motiva o investimento em controles de segurança para seus ambientes corporativos (**intranet**).

# Segurança da Informação

## AMEAÇAS À SEGURANÇA



**Razões relacionadas à perda de dados**:

- **Fatores naturais**: incêndios, enchentes, terremotos, e outros;
- **Erros de hardware ou de software**: falhas no processamento, erros de comunicação, ou bugs em programas;
- **Erros humanos**: entrada de dados incorreta, montagem errada de disco ou perda de um disco.

# Segurança da Informação

## AMEAÇAS À SEGURANÇA



Razões relacionadas à perda de dados:

- Fatores naturais
- Erros de hardware ou de software
- Erros humanos
- Para evitar a perda destes dados:
  - Podemos utilizar  oque ?????

# Segurança da Informação

## AMEAÇAS À SEGURANÇA



Razões relacionadas à perda de dados:

- Fatores naturais
- Erros de hardware ou de software
- Erros humanos
- Para evitar a perda destes dados:
  - Podemos utilizar mecanismos de backup confiável
  - Armazenado geograficamente distante dos dados originais.


# Níveis de SEGURANÇA

# Segurança da Informação

## NÍVEIS DE SEGURANÇA



**O nível de seg. deve levar em consideração**:

- ✓ os custos associados aos ataques e os associados à implementação de mecanismos de proteção;
- ✓ o quanto de deve minimizar a probabilidade de ocorrência de um ataque.
- ✓ Recomenda-se que o custo do controle não supere o valor do Ativo;
- ✓ Salvo quando a perda do ativo pode levar a processos judiciais e/ou envolver a credibilidade.

# Segurança da Informação

## NÍVEIS DE SEGURANÇA



**Segurança Física considera**:

- ✓ incêndios, desabamentos, relâmpagos, alagamento (tudo que possa gerar danos à parte física)
- ✓ o acesso indevido (controle de acesso);
- ✓ forma de tratamento e manuseio dos dados em transito.

# Segurança da Informação

## NÍVEIS DE SEGURANÇA



**Segurança Lógica considera**:

- ✓ ameaças ocasionadas por vírus;
- ✓ acessos remotos, ou não, ao ambiente e sistemas;
- ✓ backup desatualizados e/ou não certificados;
- ✓ violação de senhas, furtos de identidades, etc;
- ✓ proteção do sistema operacional;
- ✓ proteção contra sistemas com erro;
- ✓ remoção e/ou danificação de arquivos;

# Controles de SEGURANÇA

# Segurança da Informação

## CONTROLES DE SEGURANÇA



Após identificar os riscos, os níveis de proteção e determinar as perdas que os riscos podem causar, deve-se determinar os controles que serão implementados para mitigar riscos

# Segurança da Informação

## CONTROLES DE SEGURANÇA



**Macro controles da ISO/IEC 27002:**

- ✓ Política de Segurança da Informação;
- ✓ Organização da Segurança da Informação;
- ✓ Gestão e controle de ativos;
- ✓ Segurança em recursos humanos;
- ✓ Segurança física e do ambiente;
- ✓ Gestão das operações e comunicações;
- ✓ Controle de acessos;
- ✓ Aquisição, desenvolvimento e manutenção de sistemas de informação;
- ✓ Gestão da continuidade do negócio;
- ✓ Conformidade legal.

# Segurança da Informação

## CONTROLES DE SEGURANÇA



**A política de Segurança da Informação**:

- ✓ Consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos ativos de uma organização.
- ✓ Devem focar na implementação realista
- ✓ Deve definir claramente as áreas de responsabilidade dos utilizadores.
- ✓ Deve adaptar-se a alterações na organização.

# Segurança da Informação

## CONTROLES DE SEGURANÇA



**A política de Segurança da Informação**:

- ✓ Deve fornecem orientações sobre a implementação de mecanismos de segurança
- ✓ Deve definir os procedimentos de segurança, os processos de auditoria à segurança
- ✓ Deve estabelecer uma base para procedimentos legais quando da ocorrência de violações.

# Segurança da Informação

## CONTROLES DE SEGURANÇA



**A política de Segurança da Informação**:

- ✓ Não deve focar nos os aspectos técnicos de implementação dos mecanismos de segurança;
- ✓ Deve ser de fácil leitura e compreensão, além de resumido.
- ✓ O processo de escrita deste documento deve ser realizado por um grupo multidisciplinar.

# Segurança da Informação

## CONTROLES DE SEGURANÇA



Há **duas filosofias** associadas às Política de Seg.:

- A proibitiva (tudo que não é expressamente permitido é proibido)
- A permissiva (tudo que não é proibido é permitido)

# Segurança da Informação

# PÓS EM COMÉRCIO EXTERIOR E ESTRATÉGIA

## UNIVERSIDADE CATÓLICA DE PETRÓPOLIS

## CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

# TECNOLOGIA DA INFORMAÇÃO

# .:UNIDADE 05 - SEGURANÇA DA INFORMAÇÃO:.

# PARTE 1 – INTRODUÇÃO E CONCEITOS

VERSÃO: SETEMBRO DE 2018

Professor: Luís Rodrigo de O. Gonçalves

E-mail: luis.goncalves@ucp.br
Site: http://lrodrigo.sgs.lncc.br