SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2020/21

SEGURANÇA DA INFORMAÇÃO

E NORMAS APLICÁVEIS

LUIS AMORIM

13 Mar 2021

2 INTRODUÇÕES

- Nome
- Proveniência
- Conhecimentos em Segurança da Informação
- Experiência prática
  - Segurança
- Expectativas

3 INFORMAÇÕES SOBRE A CADEIRA

- Objectivos

- Aprender a projetar e orientar o desenvolvimento de uma política de segurança na organização

- Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação

- Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados

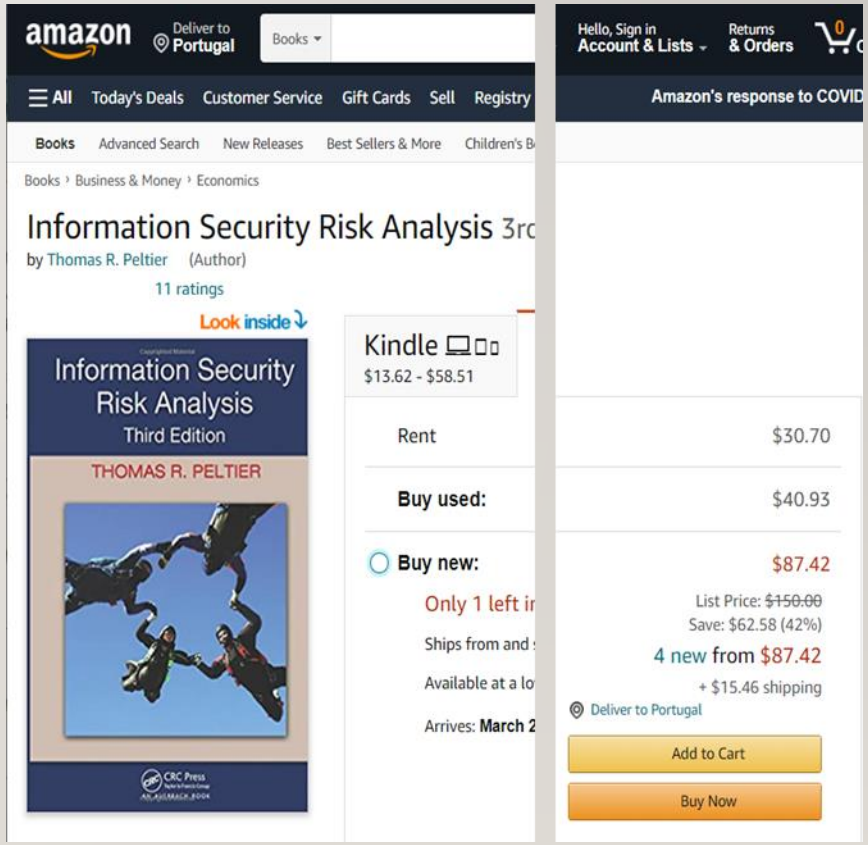
4 INFORMAÇÕES SOBRE A CADEIRA

- Bibliografia principal:
  - Information Security Risk Analysis, 3rd Edition, Thomas R. Peltier, Auerbach Publications, 2010, ISBN-978-1-4398-3956-0
  - Normas ISO 27001 e 27005
  - Publicações NIST

- Avaliação
  - Componente teórica: Teste de avaliação
  - Componente prática: Trabalho prático sobre um caso ...

5 INFORMAÇÕES SOBRE A CADEIRA

- Bibliografia principal:
  - Information Security Risk Analysis, 3rd Edition, Thomas R. Peltier, Auerbach Publications, 2010, ISBN-978-1-4398-3956-0



6 INFORMAÇÕES SOBRE A CADEIRA

- Bibliografia principal:
  - Information Security Risk Analysis, 3rd Edition, Thomas R. Peltier, Auerbach Publications, 2010, ISBN-978-1-4398-3956-0

7 INFORMAÇÕES SOBRE A CADEIRA

- Calendarização
  - Semanal, das 13 às 16, enquanto remotamente
  - Quinzenal, aos sábados, a partir de meados de Abril (??)

8 AGENDA

- Segurança da Informação
- Abordagem integrada à Segurança

9 AGENDA/OBJECTIVOS

- Capacidades/Objectivos a adquirir
  - **Compreender os princípios subjacentes à segurança nos SI**
  - **Compreender os conceitos de ameaça, a avaliação dos bens, os activos de informação, segurança física, operacional e da informação e como eles estão relacionados**
  - Compreender a análise de risco e gestão de riscos
  - Compreender as abordagens de mitigação técnicas e administrativas
  - Compreender a necessidade de um modelo de segurança global e suas implicações para o gestor de segurança
  - Compreender as tecnologias de segurança
  - Compreender as noções básicas de criptografia, as considerações sobre a sua implementação e a gestão de chaves
  - Aprender a projectar e orientar o desenvolvimento de uma política de segurança na organização
  - Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação
  - Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados

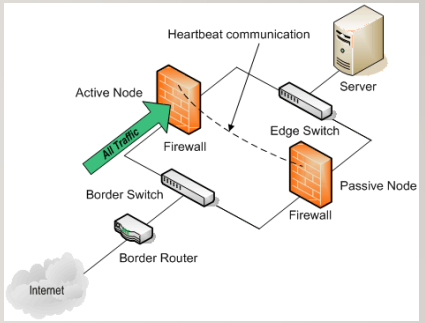
10 AGENDA

- **Segurança da Informação**

- Abordagem integrada à Segurança

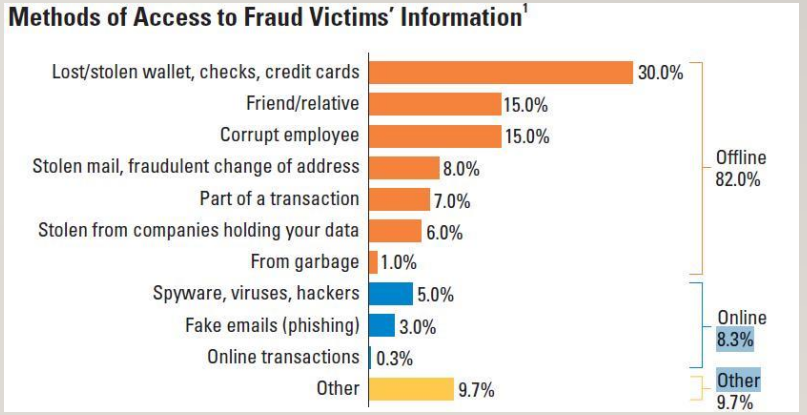
II SEGURANÇA DA INFORMAÇÃO

- Segurança dos Sistemas de Informação?



- Ou Segurança da Informação?

- Mas atualmente os Sistemas são a base da Informação…



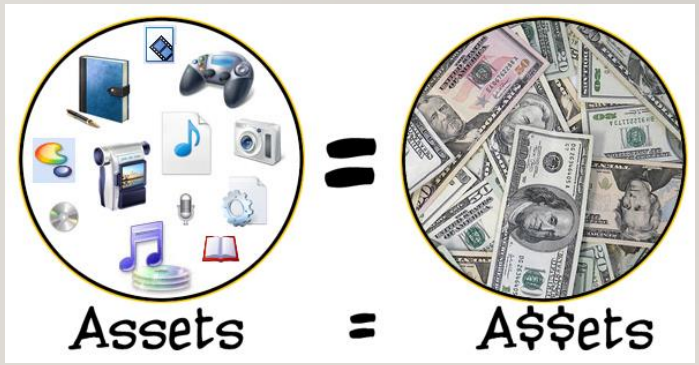
12 SEGURANÇA DA INFORMAÇÃO

- Dados vs Informação

- Os **dados** são representações de factos, conceitos ou instruções de uma maneira normalizada que se adapte à comunicação, interpretação e processamento pelo ser humano ou através de sistemas automatizados.
- Os **dados** são representados por símbolos como por exemplo as letras ou números : a, b, 1, 2 etc, mas não constituem por si informação útil.
- **Informação** é todo o conjunto de **dados** devidamente ordenados e organizados de forma a terem significado.
- A **informação** é actualmente considerada o activo mais importante nas Organizações

13 SEGURANÇA DA INFORMAÇÃO

- Importância da **Informação como activo** das organizações
- Bancos (património dos clientes)
- Forças militares (defesa nacional)
- Indústria (segredos industriais)
- Saúde (registos clínicos dos pacientes)
- Forças de Segurança (cadastro e registo de infracções)
- Transportes (operacionalidade da rede)
- E-commerce (manutenção do negócio)
- ...



14 SEGURANÇA DA INFORMAÇÃO

- Identificação de formas de Informação

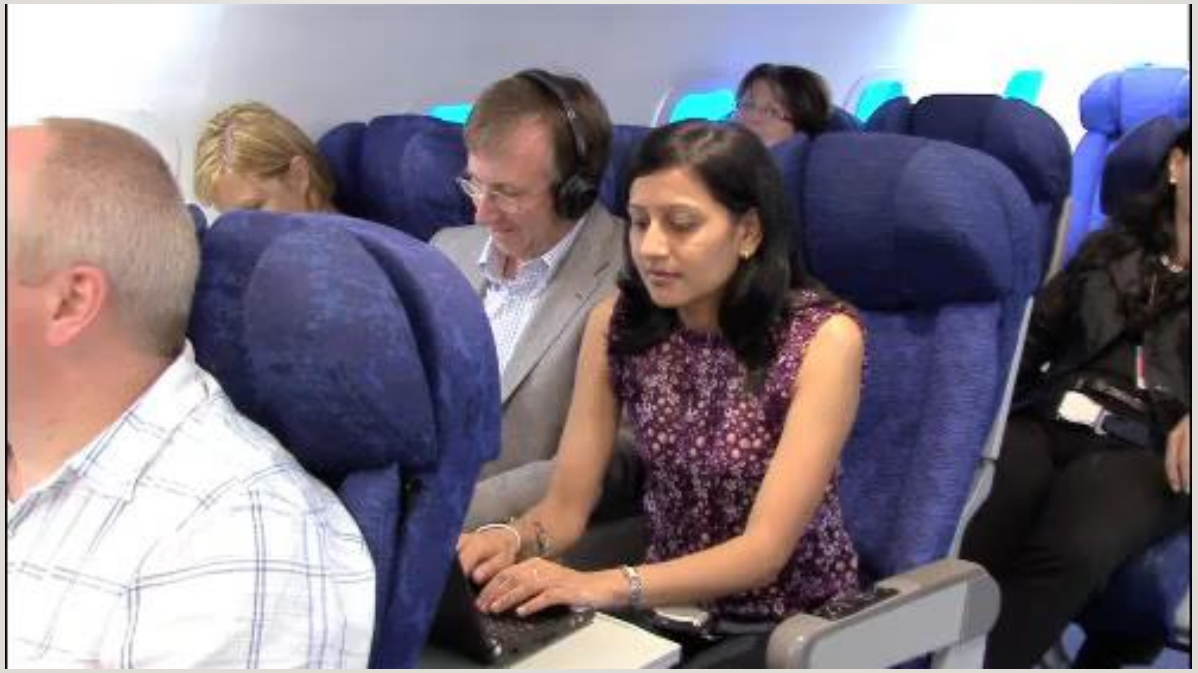
- Para se proteger a informação temos que começar por identificar as formas pelas quais essa informação é veiculada
  - Visual
  - Áudio
  - Escrita
  - ....
  - Electrónica

SEGURANÇA DA INFORMAÇÃO
FORMAS DA INFORMAÇÃO - A INFORMAÇÃO VISUAL/MULTIMEDIA

- Informação capturada por câmaras
  - Cuidados acrescidos face à mediatização de certos eventos
  - E à proliferação de meios como CCTV

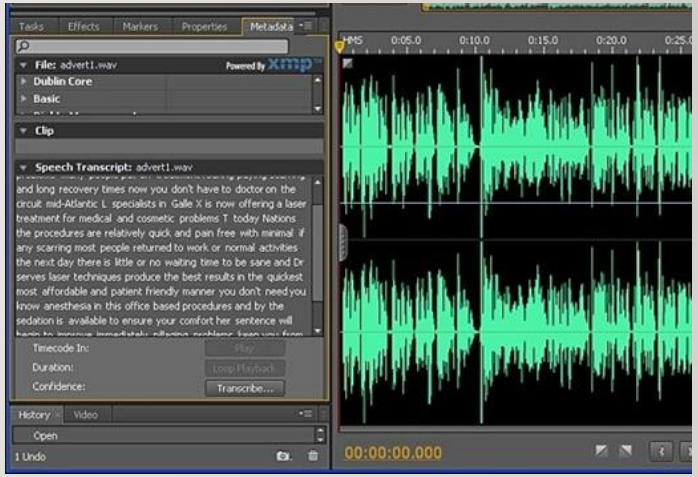
- Informação em locais públicos
  - Avião/Transportes públicos
  - Locais públicos

16 SEGURANÇA DA INFORMAÇÃO
FORMAS DA INFORMAÇÃO - A INFORMAÇÃO VISUAL/MULTIMEDIA



SEGURANÇA DA INFORMAÇÃO
FORMAS DA INFORMAÇÃO - A INFORMAÇÃO POR VIA ORAL/ÁUDIO

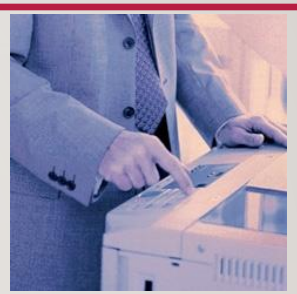
- Sistemas de análise de informação
  - Permitem investigação
    (tal como permitem espionagem)
  - Permitem também a autenticação e
    controlo de acesso



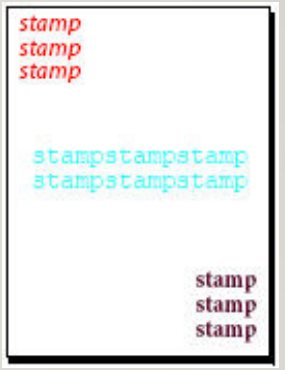
- Sistema de encriptação de voz
  - Protegendo a comunicação

SEGURANÇA DA INFORMAÇÃO
FORMAS DA INFORMAÇÃO - A INFORMAÇÃO IMPRESSA

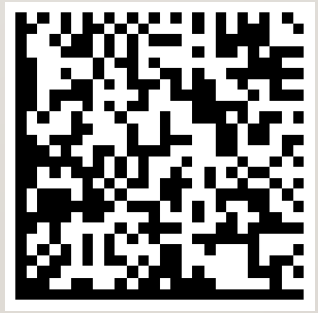
- Controlo de impressão
  - Secure printing



- Controlo das cópias impressas
  - Accounting
  - Stamping / Watermarking (com certificação temporal) de documentos

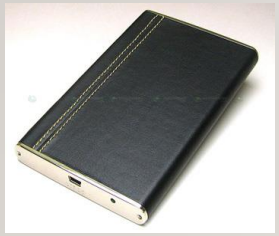


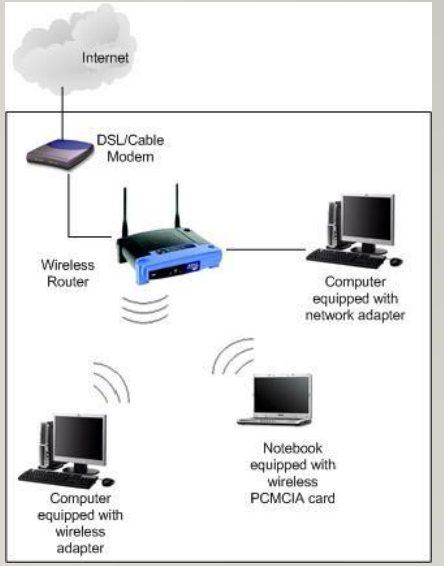
- Proteção da informação impressa
  - Dados sensíveis encriptados



19 SEGURANÇA DA INFORMAÇÃO
FORMAS DA INFORMAÇÃO - A INFORMAÇÃO IMPRESSA

SEGURANÇA DA INFORMAÇÃO
FORMAS DA INFORMAÇÃO - A INFORMAÇÃO EM FORMATO DIGITAL





- Algumas formas de proteger
  - Discos cifrados (bitlocker)
  - Comunicação segura (VPV)
  - Segregação de redes (VLANs)

SEGURANÇA DA INFORMAÇÃO - CONTROLO DE ACESSO À INFORMAÇÃO

- Âmbito da informação
  - Interna
  - Parceiros
  - Clientes
  - Pública
  - …
- Classificação
  - Não classificada
  - Reservada
  - Confidencial
  - …
- Atenção: Tanto o âmbito como a classificação podem variar ao longo do tempo <> processo de gestão

22 SEGURANÇA DA INFORMAÇÃO

- Information Security [ISO/IEC 27001]

- "Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved"

23 SEGURANÇA DA INFORMAÇÃO

- C-I-A - As três características essenciais para a segurança da informação
- C – Confidentiality
  "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes"

- I – Integrity
  "The property of safeguarding the accuracy and completeness of assets"

- A – Availability
  The property of being accessible and usable upon demand by an authorized entity

- Para cada organização, cada uma destas características pode ter um peso diferente
- Banca ≠ Eléctrica ≠ Transportes ≠ Saúde

SEGURANÇA DA INFORMAÇÃO

- **A gestão da Segurança de Informação na Organização visa**
  - Garantir a preservação da confidencialidade, integridade e disponibilidade da informação;
  - Reduzir os riscos para o negócio prevenindo e minimizando os impactos dos incidentes de segurança;
  - Assegurar a Continuidade do Negócio da Organização.

- **Information Security Management System (ISMS)**
  - "That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security"; [ISO/IEC 27001]
  - É um processo de gestão;
  - Não se resume à componente tecnológica, mas esta faz parte do processo de gestão da segurança

SEGURANÇA DA INFORMAÇÃO

- **Conceitos**
  - Ameaça - Threat

    Uma ameaça é qualquer coisa (acto humano intencional ou não, ou causada pela natureza), que tem o potencial de causar danos

  - Vulnerabilidades - vulnerability

    A vulnerabilidade é uma fragilidade que pode ser usada para colocar em perigo ou causar danos a um ativo de informação

  - Riscos - Risk

    Risco é a probabilidade de algo mau vir a acontecer e causar danos a um activo de informação

- **A probabilidade de uma ameaça vir a usar uma vulnerabilidade, para causar dano, resulta num risco para a organização.**

26 SEGURANÇA DA INFORMAÇÃO

- Ameaças
  - Vandalismo
  - Terrorismo
  - Hacking
  - Espionagem
  - Terramoto
  - Inundação
  - Avaria
  - Falha de energia
  - Pandemia
  - …

27 SEGURANÇA DA INFORMAÇÃO

- Vulnerabilidades
  - Inexistência de Firewall
  - Inexistência de IDS/IPS
  - Atraso na implementação de actualizações de segurança
  - Sistemas não Redundantes
  - Informação em claro
  - Não utilizar VPNs nas ligações remotas
  - Fraca política de autenticação
  - Falta de formação/sensibilização dos colaboradores
  - …

SEGURANÇA DA INFORMAÇÃO

- Riscos
  - Roubo de Informação
    - Ou Roubo de informação, deixada sobre a secretária, por uma visita externa – Porquê?
  - Perda de dados
  - Corrupção de dados
  - Personificação
  - Denial of service
  - ...

  Mas também os Riscos associados a
  - Documentos em suporte físico (papel):
    - Nas secretárias;
    - Nos caixotes de lixo;
    - Nas fotocopiadoras/impressoras.
  - Informação deixada em quadros e flipcharts
  - Telefones/PDAs com informação valiosa
  - Conversas em locais públicos

SEGURANÇA DA INFORMAÇÃO

- A Segurança da informação deve ser um processo integrado, que abrange toda a organização

EXEMPLIFICAÇÃO

- Segurança da Informação

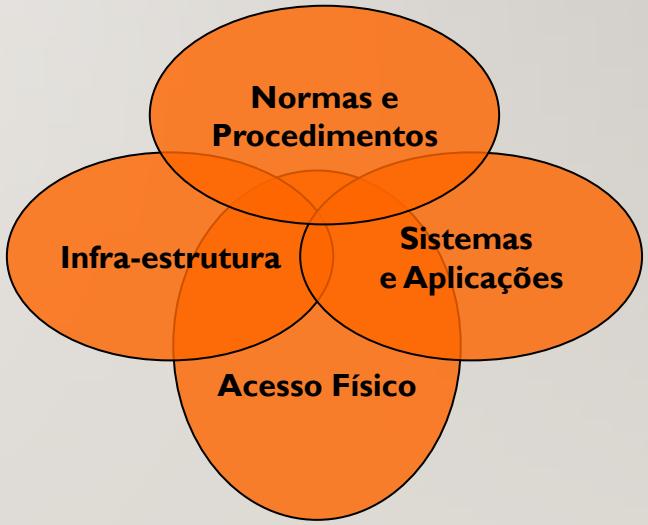
31 AGENDA

- Segurança da Informação

- **Abordagem integrada à Segurança**

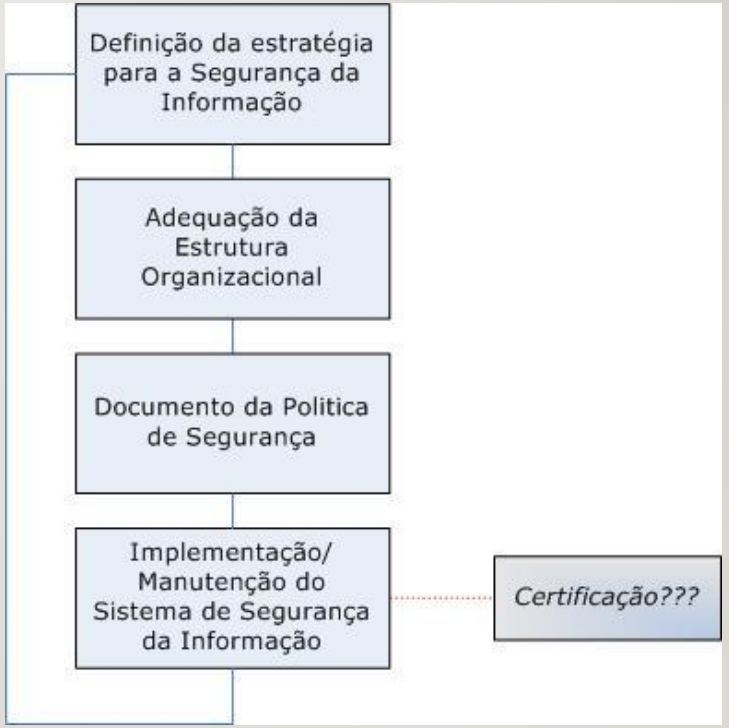
32 ABORDAGEM INTEGRADA À SEGURANÇA

- A Segurança de um Sistema de Informação só se consegue atingir considerando de forma integrada:
  - Normas e Procedimentos
    - Definição adequada de processos de negócio e fluxos de trabalho
    - **Definição de Políticas de Segurança**
    - Definição de Processo de Desenvolvimento de Software
    - Procedimentos de Operação definidos (operacionalização)
    - Programas de Sensibilização
  - Sistemas e Aplicações
    - Devidamente testados
    - Acompanhados ao longo do ciclo de vida
  - Infra-estrutura
    - Adequada aos Sistemas e Aplicações
    - Mecanismos de controlo (firewalls, ids ...)
    - Mecanismos de monitorização
  - Acesso Físico
    - Acesso ao(s) edifício(s)
    - Controlo de acesso a zonas
    - Monitorização



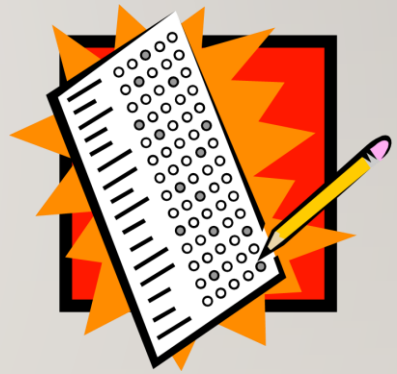
ABORDAGEM INTEGRADA À SEGURANÇA

- Roadmap para Política de Segurança



34 ABORDAGEM INTEGRADA À SEGURANÇA

- Definição da Estratégia para a Segurança da Informação
  - Âmbito
    - O que se pretende proteger?
    - Registos informáticos
    - Papel
    - Espaço Físico...
  - Requisitos da Política de Segurança
    - A política de segurança deve ser caracterizada pela preservação da:
    - Confidencialidade da informação;
    - Integridade da informação;
    - Disponibilidade da informação;
    - Requisitos contratuais, regulamentares, estatutários e legais
  - Outras linhas orientadoras
    - Identificação dos riscos
    - Conjunto de princípios, objectivos e requisitos para ao processamento da informação necessários para o negócio

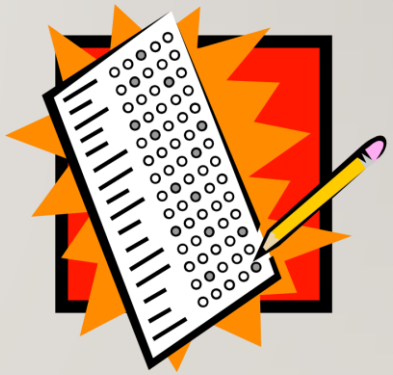


35 ABORDAGEM INTEGRADA À SEGURANÇA

- Adequação da Estrutura Organizacional
  - Comité de gestão da segurança da informação
    - Identificação dos elementos
    - O comité de gestão da segurança da informação deverá ser constituído por elementos da gestão de topo e por elementos com responsabilidade a nível operacional.
    - Missão e responsabilidades
    - Revisão e aprovação da política de segurança da informação;
    - Definição de responsabilidades no âmbito da política de segurança da informação;
    - Revisão e monitorização dos incidentes de segurança da informação;
    - Aprovação das iniciativas relacionadas com a segurança da informação.

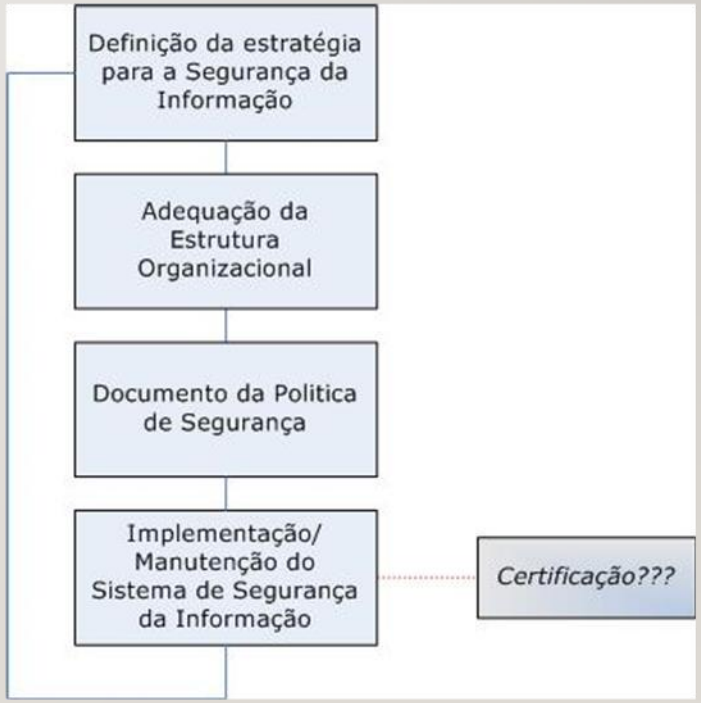
36 ABORDAGEM INTEGRADA À SEGURANÇA

- Política de Segurança
  - A Política deve focar
    - Segurança Organizacional
    - Conformidade com requisitos regulamentares, legais, etc;
    - Controlo de acessos, comunicações e dados;
    - Procedimentos para a classificação da informação;
    - Procedimentos e responsabilidades operacionais;
    - Requisitos de segurança para manutenções e novos desenvolvimentos;
    - Planos de continuidade de negócio
  - Importante garantir o alinhamento da Política de Segurança
    - Auditorias internas/externas
    - Análise dos relatórios de incidentes
    - Alterações dos requisitos de negócio



37 ABORDAGEM INTEGRADA À SEGURANÇA

- Roadmap para Política de Segurança



SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2020/21

SEGURANÇA DA INFORMAÇÃO

E NORMAS APLICÁVEIS

LUIS AMORIM

13 Mar 2021