Segurança da Informação...

JORNADAS COMPUTAÇÃO CIENTÍFICA 2018 INL 11-13 ABRIL

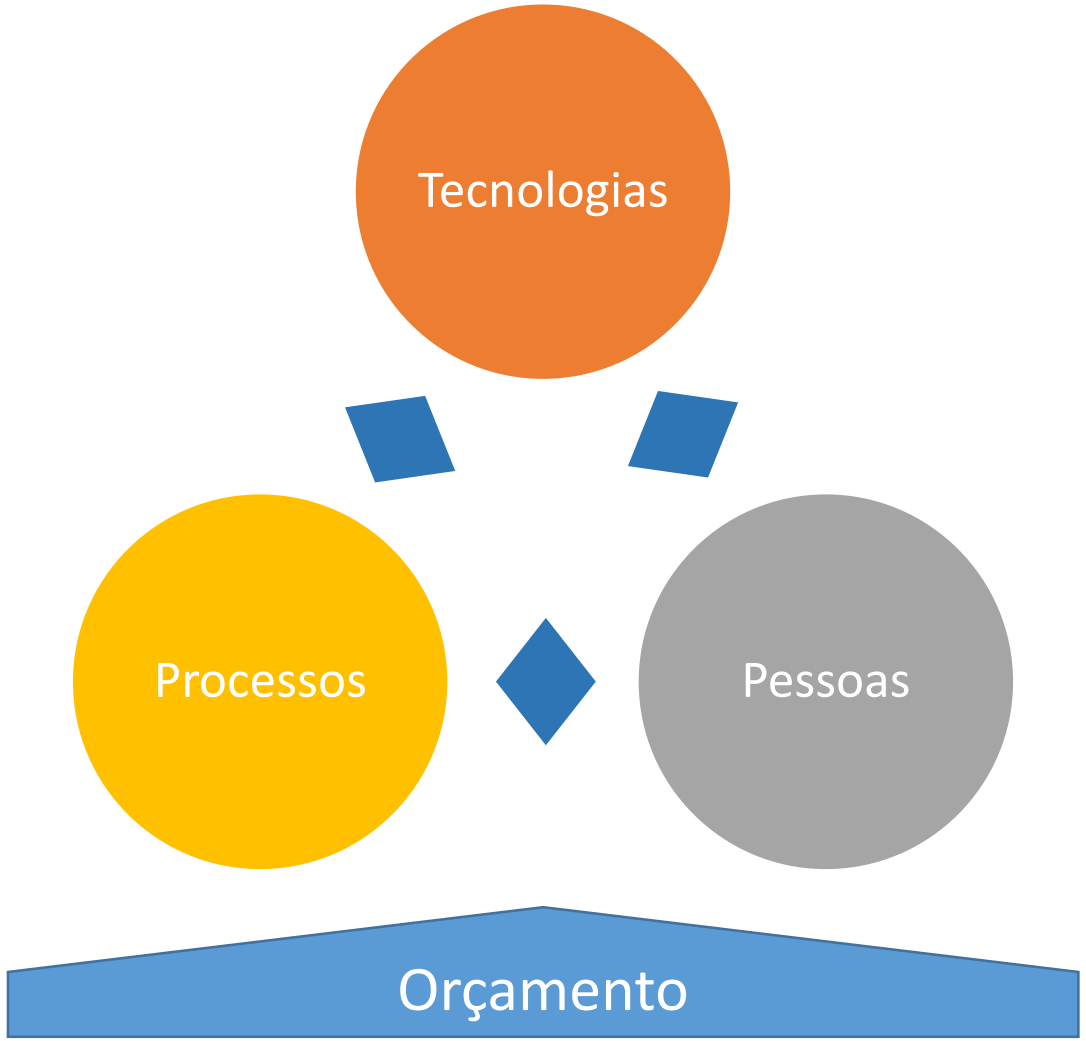
PORTUGAL INCoDe.2030

...nas Instituições de Ensino Superior

Universidade de Aveiro | Ricardo T. Martins
ricardo@ua.pt | 2018 / 04 / 13

universidade de aveiro
theoria poiesis praxis

Gestão da Segurança da Informação: Sistema



Ponto de Situação

- Temos implementado algum sistema de gestão da segurança da informação?
- Temos algumas medidas de proteção implementadas?
- Temos uma equipa de segurança?

Sistema Integrado de Gestão de Serviços e de Segurança da Informação

- Catálogo de Serviços
- Gestão de Alterações
- Gestão de Entregas
- Gestão de Ativos e Configurações
- Gestão de Pedidos de Serviço
- Gestão de Incidentes
- Orçamentação e Contabilização
- Gestão da Capacidade
- Gestão da Relação com Negócio
- Gestão de Fornecedores
- Gestão da Continuidade e Disponibilidade
- Gestão da Segurança da Informação
- Gestão de Incidentes de Segurança

ISO/IEC 27001:2013

- É um sistema de gestão integrado e holístico (vai além do RGPD);
- Exigente do ponto de vista da organização;
- Garante um elevado nível de proteção da informação;
  - Processual e procedimental;
  - Tecnológico;
- Garante o reconhecimento externo dos processos de gestão da segurança da informação;
- Impossível de implementar só por técnicos.
- Implica a organização (reitoria/administração/serviços)

Questão:

Podemos alinhar todos pela ISO/IEC 27001?

Conceitos

Security by Design

- Privilégios mínimos;
- Perfil seguro por omissão;
- Economia do desenho (tão simples quanto possível);
- Concessão de acesso apenas após validação prévia;
- Desenho aberto;
- Separação de privilégios (multiplas condições para o acesso);
- Aceitação psicológica;
- Defesa em profundidade (múltiplas camadas);

- https://dzone.com/articles/9-software-security-design

Privacy by Design

- Proativo e não Reativo; Preventivo e não remediativo
- Privacidade por pré-definição
- Pivacidade embebida no desenho
- Funcionalidade total – sem comprometer a Segurança
- Segurança fim-a-fim (como um ciclo)
- Visibilidade e transparência
- Respeito pela privacidade do utilizador (titular)

- https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
- https://gpsbydesign.org/

Questão:

Faz sentido partilhar como estamos a implementar estes princípios?

Gestão de Identidades

Gestão de Identidades e acessos privilegiados

- Existe um processo automático de IdM?
- Separamos as contas de utilizador de contas de administração?
- Privilégios mínimos (os estritamente necessários)?
- Políticas de autenticação com duplo fator?
- Registo e auditoria das operações de gestão?

Desenvolvimento de Software

Ambientes: Desenvolvimento, QA e Produção

Desenvolvimento

- Produção de Código
- Security by Design
- Testes Unitários

- Dados: dummy

Quality Assurance

- Testes Funcionais
- Testes de Interface
- Testes de Segurança
- Testes de Desempenho
- Teste de Integração

- Dados: pseudonimizados

Produção

- Testes de Segurança
- Testes de Desempenho
- Bug free

- Dados: reais

Guidelines: produção de código

- Controlo automático de versões (GIT)
- Realização de testes unitários
- Realização de auditorias de código fonte (*static/source code analysis*; Ex: veracode, fortify)
- OWASP (Open Web Application Security Project)

OWASP: Top 10

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure
- A4:2017-XML External Entities (XXE)
- A5:2017-Broken Access Control
- A6:2017-Security Misconfiguration
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization
- A9:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging&Monitoring

Podemos cooperar?

Trabalho em Rede

- Repositório aberto à RCTS:
  - Políticas
  - Procedimentos
  - Templates
- "Blog/Wiki" para partilha de informação sobre falhas e/ou incidentes de segurança, com o que fizemos em termos de remediação;
- Cadernos de encargos "partilhados"?
- Partilha de experiências e documentos sobre a implementação do RGPD.

Financiamento

Financiamento

- Sistema de apoio à modernização e capacitação da administração pública (SAMA2020)

- https://www.ama.gov.pt/web/agencia-para-a-modernizacao-administrativa/projetos-sama-ama

Obrigado!

universidade de aveiro
theoria poiesis praxis

JORNADAS COMPUTAÇÃO CIENTÍFICA 2018 INCD 11-13 ABRIL