Workshop ANACOM – itSMF Portugal
Normalização de TI – técnicas de segurança

Lisboa, 19 de Dezembro, 2012

Trabalho desenvolvido pela CT 163

2004 a 2011

Henrique Santos

Centro Algoritmi/Universidade do Minho

Sumário

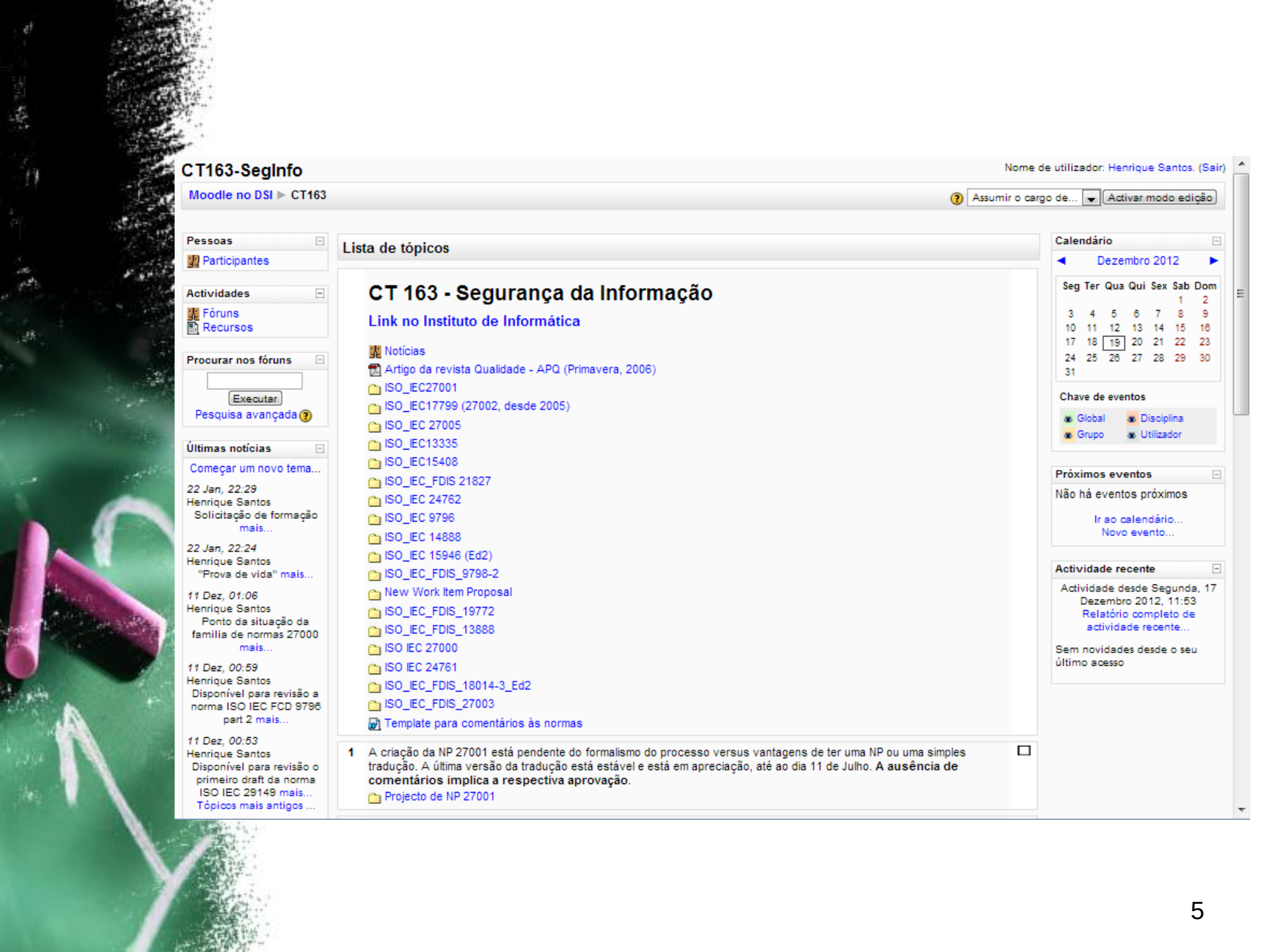
- Historial
- Acompanhamento da normalização
- Tradução portuguesa da ISO 27001
- Proposta de uma *framework* para a CT
- Conclusões

Historial

- Data de criação: 23/11/2004
  - Por iniciativa do InstInf (como ONS) e do IPQ (como ONN)
  - Foi criada a CT, com a designação: **Técnicas de Segurança para Sistemas de Informação**
  - E com o âmbito de actuação: **Normalização de técnicas e métodos de segurança em SI**
  - Tendo como principal objectivo: **Acompanhamento das actividades relevantes desenvolvidas pelos organismos internacionais, nomeadamente: ISO/IEC (JTC 1, SC 27) e congéneres europeus**
  - **7 vogais, 4 dos quais dos promotores e 3 externos (UM, GNS, Sun)**

Historial

- Em 2008 a CT-163 contava com a participação de 24 vogais:
  - Instituições de Ensino Superior (UM, ESTG/IPL e ESTSC)
  - Organizações estatais (InstInf, IPQ, GNS, ITIJ)
  - Empresas (Sun, BitOrder,Vodafone, Sinfic, Link, Ogimatech, Microsoft, Multicert, Montepio, IBM)
- Cerca de 2 reuniões anuais
- Acompanhamento das normas no seu processo de aprovação (apoio logístico do InstInf)
- Foi criada uma plataforma Moodle para suporte ao trabalho colaborativo
- Discutia-se o estatuto da CT 163 (P/O)


CT163-SegInfo
Nome de utilizador: Henrique Santos. (Sair)
Moodle no DSI ▶ CT163
Assumir o cargo de...
Activar modo edição
Pessoas
Participantes
Actividades
Fóruns
Recursos
Procurar nos fóruns
Executar
Pesquisa avançada
Últimas notícias
Começar um novo tema...
22 Jan, 22:29
Henrique Santos
Solicitação de formação
mais...
22 Jan, 22:24
Henrique Santos
"Prova de vida" mais...
11 Dez, 01:06
Henrique Santos
Ponto da situação da família de normas 27000
mais...
11 Dez, 00:59
Henrique Santos
Disponível para revisão a norma ISO IEC FCD 9796 part 2 mais...
11 Dez, 00:53
Henrique Santos
Disponível para revisão o primeiro draft da norma ISO IEC 29149 mais...
Tópicos mais antigos ...
Lista de tópicos
CT 163 - Segurança da Informação
Link no Instituto de Informática
Notícias
Artigo da revista Qualidade - APQ (Primavera, 2006)
ISO_IEC27001
ISO_IEC17799 (27002, desde 2005)
ISO_IEC 27005
ISO_IEC13335
ISO_IEC15408
ISO_IEC_FDIS 21827
ISO_IEC 24762
ISO_IEC 9796
ISO_IEC 14888
ISO_IEC 15946 (Ed2)
ISO_IEC_FDIS_9798-2
New Work Item Proposal
ISO_IEC_FDIS_19772
ISO_IEC_FDIS_13888
ISO IEC 27000
ISO IEC 24761
ISO_IEC_FDIS_18014-3_Ed2
ISO_IEC_FDIS_27003
Template para comentários às normas
1 A criação da NP 27001 está pendente do formalismo do processo versus vantagens de ter uma NP ou uma simples tradução. A última versão da tradução está estável e está em apreciação, até ao dia 11 de Julho. A ausência de comentários implica a respectiva aprovação.
Projecto de NP 27001
Calendário
Dezembro 2012
Seg Ter Qua Qui Sex Sab Dom
1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
Chave de eventos
Global
Disciplina
Grupo
Utilizador
Próximos eventos
Não há eventos próximos
Ir ao calendário...
Novo evento...
Actividade recente
Actividade desde Segunda, 17 Dezembro 2012, 11:53
Relatório completo de actividade recente...
Sem novidades desde o seu último acesso

Acompanhamento da normalização

- Até 2008 chegavam à CT entre 10 a 20 normas por ano, que eram distribuídas por todos os membros
  - Mais abrangentes (*frameworks*)
    - Família 27000, 13335, 15408, 18028, 19785, 20000, 24760, 29100
  - Mais específicas
    - Técnicas criptográficas (…)
    - Deteção de intrusões (18043)
    - *Disaster Recover* (24762)
    - …
  - BSi 17799, 7799, 25999
  - Número de comentários praticamente nulo ☹

Acompanhamento da normalização

- Em 2009 o InstInf renuncia ao seu papel de ONS
- O IPQ continua a reencaminhar a informação relevante (SC27), mas de uma forma não estruturada, o que compromete muito o funcionamento da CT
- O último *roadmap* do SC27/WG1 recebido: 2010 (demonstrava o enfoque do SC 27 na família de normas 27000)
- O último documento normativo recebido data de 3/1/2011
- A CT sessou a atividade (de forma não formal) em Janeiro de 2011

Tradução portuguesa da ISO 27001

- Processo desencadeado por um vogal (Paulo Coelho), em 2007
- Revisão interna baseada numa plataforma colaborativa (Moodle), terminou em Junho de 2008
- Processo de publicação não concluído ☹
  - Razões internas (dinâmica da CT)
  - Razões externas (enquadramento desfavorável)

Proposta de uma *framework* para a CT 163

- Limitações
  - Estatuto de voluntariado impede um envolvimento mais formal com a SC 27 e outros grupos de trabalho afins
  - Estímulo externo é limitado, refletindo-se no benefício percecionado
  - Falta de hábitos neste tipo de trabalho
- Potencialidades
  - Pluralidade de ideias e natureza aberta do grupo
  - Área com uma crescente necessidades de normalização (esfera política…)
  - Novo enquadramento institucional (itSMF Portugal)
  - Espaço normativo em língua portuguesa

Proposta de uma *framework* para a CT 163

- Foco nas normas mais abrangentes, seguindo naturalmente o *roadmap* do SC 27
  - 27000 (Segurança da Informação)
  - 15408 (Avaliação da Segurança)
  - 18028 (Segurança em Redes)
  - 24760 (Sistemas de Gestão de Identidades)
  - …
- Organização de subgrupos (garantido a pluralidade) mais específicos do que os “WG” – e.g., técnicas criptográficas
- Maior estímulo ao recurso a plataformas colaborativas (Moodle, Skype,…)
- Organização de um workshop anual
- Maior envolvimento com as atividades do SC 27 e grupos afim – SC 37 (Biometrias); TC 68 (*Banking*); TC 215 (*Healthcare*); TC 65 (*Safety*); ISSEA; ISSA; ITU-T

Conclusões

- Experiência de trabalho enriquecedora, mas por vezes frustrante
- Enquadramento institucional é fundamental
- Contexto atual muito favorável
- Organização dos processos pode ser melhorada
- Mas há duas questões a responder:
  - Até onde queremos ir (WG1/2/3)?
  - Até onde podemos ir?