Certificação de repositórios

SOS Digital // Preservação comum de património digital

18 Junho 2014 // Arquivo Nacional Torre do Tombo

Miguel Ferreira, PhD.
Director executivo // KEEP SOLUTIONS
mferreira@keep.pt

KEEPSOLUTIONS
University of Minho SPIN-OFF

Porquê certificar um repositório digital?

Estabelecer um clima de confiança em torno do repositório
Informação que nele se encontra custodiada
Produtores, Consumidores, Gestores, Operadores, Financiadores, etc.

Capacidade de demonstrar e medir de forma objetiva que o nosso repositório é de confiança

Postura de transparência perante todos os intervenientes

Demonstrando que existem procedimentos e que estes são seguidos
com base em evidências

Quantos de vocês confiam nos sistemas de informação da Segurança Social?

Serão estes sistemas capazes de preservar os vossos registos durante 20, 30 ou 40 anos?

Já imaginaram quantos governos, políticas e sistemas de governação estes registos terão de atravessar?

Já imaginaram quantos sistemas de informação, tecnologias, arquiteturas de hardware, etc., os vossos registos irão encontrar?

A derradeira questão é

Quantas pessoas terá a Segurança Social a pensar nestas questões?

Instrumentos de auditoria e certificação

DRAMBORA

Digital Repository Audit Method Based on Risk Assessment

Desenvolvido pelo Digital Curation Centre (DCC) e pelo DigitalPreservationEurope (DPE)

Nasce da experiência acumulada após realizar um conjunto de auditorias ao longo do ano de 2006

- Tendo por base uma versão preliminar do TRAC

O DRAMBORA é um documento e uma ferramenta interativa que sistematiza um processo de auto-avaliação

- Foca-se mais em aspetos ligados à gestão estratégica e à organização, e menos em aspetos técnicos relacionados com o repositório e respectiva plataforma tecnológica
- Abordagem top-down
- http://www.repositoryaudit.eu/

O DRAMBORA convida os administradores de repositórios digitais a

- Elaborar um perfil organizacional, documentando a sua política de depósito, objetivos, responsabilidades, atividades e material custodiado;
- Identificar e avaliar os riscos que poderão impedir a prossecução da sua missão e que ameaçam a salvaguarda dos seus materiais;
- Gerir eficazmente os riscos, mitigando a sua probabilidade de ocorrência;
- Estabelecer planos de contingência eficazes para minimizar os efeitos provocados por riscos que não puderam ser evitados
- Relatar os resultados do processo de auto-avaliação

DSA

Data Seal of Approval

Estabelecido em 2009

"Selo de garantia" emitido por um grupo de especialistas em preservação digital

- i.e. O conselho do Data Seal of Approval

Atesta que um repositório é capaz de preservar dados científicos para futura referência e processamento

- sem que isso acarrete elevados custos ou investimentos para as entidades que os custodiam

Conjunto de boas-práticas que se pretendem que sejam seguidas por organizações responsáveis pela preservação de dados científicos

O DSA é composto por 16 requisitos

- 3 dizem respeito ao processo de ingestão
- 10 ao repositório e seus processos internos

O processo de obtenção do "selo" não requer a visita de auditores externos

- Todo o processo é conduzido em-linha
- O auditado apenas tem de apresentar evidências de que cumpre os 16 requisitos definidos
- Alguns requisitos, mas não todos, podem ser cumpridos em regime de outsourcing

Exemplos de requisitos

- O produtor deposita os seus dados no repositório com informação suficiente para que outros possam aferir a sua qualidade científica e de forma compatível com as normas éticas exigidas pela disciplina em questão?
- O repositório assegura a integridade dos dados e dos metadados sob sua custódia?
- O consumidor respeita os níveis de acesso à informação definidos pelo repositório?

Os resultados da auditoria são publicados em-linha no sítio Web do DSA

http://www.datasealofapproval.org/

ISO 16363

Audit and Certification of Trustworthy Digital Repositories

O ISO 16363 deriva do TRAC, documento publicado em 2007 pela

- RLG (Research Library Group)
- NARA (National Archives and Records Administration)

Enumera um conjunto de requisitos que vão desde a gestão organizacional às infraestruturas
visam aferir a confiabilidade de um repositório

O TRAC tornou-se uma norma ISO em 2012

- ISO/DIS 16363 – Audit and certification of trustworthy digital repositories = TRAC
- ISO/DIS 16919 – Requirements for bodies providing audit and certification of candidate trustworthy digital repositories

Os objetivos da norma são:

- Fornecer uma ferramenta que permita auditar, avaliar, e potencialmente certificar repositórios digitais
- Estabelecer a documentação necessária para realizar uma auditoria
- Delinear o processo de certificação
- Estabelecer metodologias apropriadas para determinar a robustez e a sustentabilidade de um repositório digital

A aplicação da norma potencia a confiança junto dos utilizadores do repositório pois

- Estabelece um clima de transparência relativamente aos processos implementados
- Auxilia na realização de auditorias internas e externas

Partes da norma

Estrutura organizacional (25 requisitos)

- Estrutura governativa e viabilidade organizacional (5 requisitos)
- Estrutura organizacional e recursos humanos (4 requisitos)
- Documentação de processos e políticas de preservação (7 requisitos)
- Sustentabilidade financeira (3 requisitos)
- Contratos, licenças e responsabilidades (6 requisitos)

Gestão de objetos digitais (42 requisitos)

- Ingestão: incorporação de informação digital (10 requisitos)
- Ingestão: criação do Pacote de Informação de Arquivo (AIP) (12 requisitos)
- Planeamento de preservação (6 requisitos)
- Preservação do AIP (6 requisitos)
- Gestão de informação (4 requisitos)
- Gestão de acessos (4 requisitos)

Infraestrutura e gestão da segurança (23 requisitos)

- Gestão de riscos inerentes à infraestrutura (20 requisitos)
- Gestão da segurança (3 requisitos)

Processo de auditoria

1. Autoavaliação

Os responsáveis são convidados a realizar uma autoavaliação para cada um dos requisitos do referencial normativo
Estes devem apresentar evidências do cumprimento dos vários requisitos normativos

3. Análise e avaliação

Após a receção da autoavaliação e respetivos materiais associados, a equipa auditoria analisa todas as evidências fornecidas e efetua a sua própria avaliação

4. Plano de ação

Para cada requisito cuja avaliação se situou abaixo do nível desejado, são fornecidas sugestões de melhoria
Para as avaliações que divergiram da autoavaliação são providenciados comentários que visam explicar o motivo da divergência

5. Implementação das ações

Pelos responsáveis pelos repositórios

6. Auditoria presencial

Análise detalhadas das ações implementadas

7. Relatório final

Relatório onde se resumem as principais constatações detetadas ao longo do processo de auditoria

Níveis de conformidade

Nível	Designação	Descrição
1	Inexistente	O repositório não implementa quaisquer processos que poderão ir de encontro às exigências do requisito normativo.
2	Incipiente	O repositório está consciente da necessidade de existirem processos para suprir o requisito, porém estes não se encontram devidamente formalizados ou são realizados de forma ad-hoc.
3	Em formação	O repositório possui processos definidos que satisfazem o requisito normativo, porém estes ainda não se encontram totalmente implementados e/ou disseminados.
4	Operacional	Existem políticas, procedimentos e processos implementados que satisfazem as exigências do requisito normativo.
5	Pró-ativo	Existem políticas, procedimentos e processos devidamente enquadrados num sistema de gestão que visa a monitorização e a melhoria contínua tendo por base um plano estratégico assente em factos, i.e. objetivos, metas e indicadores.

ISO 16363

Atualmente ainda não existem entidades certificadoras em Portugal segundo o

Exemplos
riscos que a norma procura mitigar

Desinteresse da gestão

Cessação de atividade da organização

Problemas com os recursos humanos
rotatividade/turnover
falta de formação
insuficiência de recursos

Ruptura financeira

Litígios ao nível dos direitos

Perda de informação
metadados, objetos, propriedades, identificadores, bitrot

Obsolescência tecnológica

Insatisfação da comunidade de interesse

Acessos indevidos

KEEPSOLUTIONS

University of Minho SPIN-OFF

ARQUIVOS | BIBLIOTECAS | MUSEUS

www.keep.pt

Miguel Ferreira
Consultor
mferreira@keep.pt