C. Technology

XV. Technical infrastructure

R15. The repository functions on wellsupported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.

Guidance:
Repositories need to operate on reliable and stable core infrastructures that maximizes service availability. Furthermore, hardware and software used must be relevant and appropriate to the Designated Community and to the functions that a repository fulfils. Standards such as the OAIS reference model specify the functions of a repository in meeting user needs.

For this Requirement, responses should include evidence related to the following questions:

● What standards does the repository use for reference? Are these international and/or community standards (e.g., Spatial Data Infrastructure (SDI) standards, OGC, W3C, or ISO 19115)? How often are these reviewed?

● How are the standards implemented? Are there any significant deviations from the standard? If so, please explain.

● Does the repository have a plan for infrastructure development? If so, what is it?

● Is a software inventory maintained and is system documentation available?

● Is community supported software in use? Please describe.

● For real-time to near real-time data streams, is the provision of around the clock connectivity to public and private networks at a bandwidth that is sufficient to meet the global and/or regional responsibilities of the repository?

Self-assessment statement:

O sistema assenta no software OpenSource DSpace, compatível com o esquema de metadados Dublin Core e protocolo OAI-PHM, instalado em Sistema Operativo OpenSource Linux, distribuição CentOS, em infraestrutura redundante e de alta disponibilidade, fornecida pela FCT|FCCN.

Evidências:

1. Informação pública sobre o Software e standards:

https://wiki.duraspace.org/display/DSPACE/Home e http://www.dspace.org/why-use

2. Sobre os standards implementados (DC, MODS, METS):

https://wiki.duraspace.org/display/DSPACE/Home e http://www.dspace.org/why-use

https://wiki.duraspace.org/display/DSDOC3x/Importing+and+Exporting+Content+via+Packages

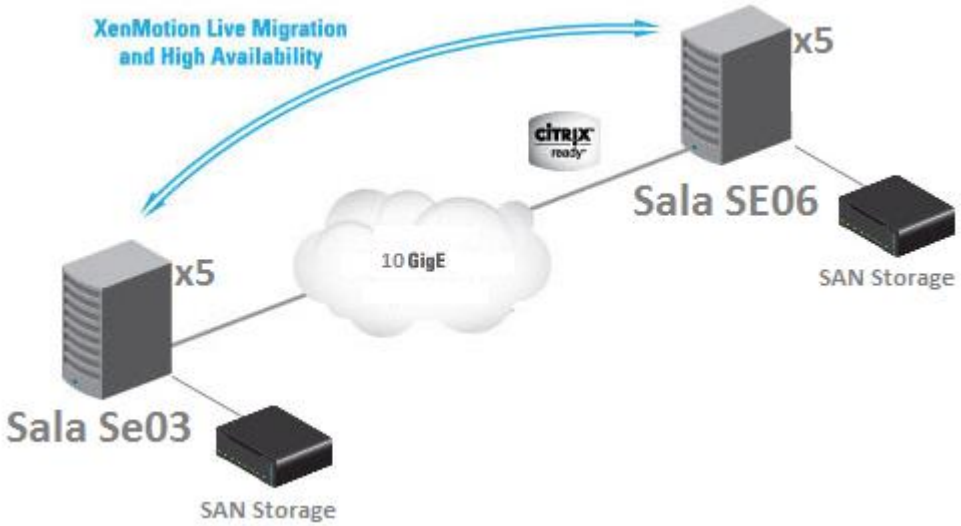
3. O repositório faz avaliações anuais de capacidade e previsões de evolução a 6 meses. As avaliações incidem sobre espaço em disco, utilização de CPU, utilização de memória e consumos de largura de banda.
4. A informação sobre o software instalado é mantida numa wiki privada ligada ao projeto. A documentação do software utilizado pode ser encontrada em https://wiki.duraspace.org/display/DSDOC3x/DSpace+3.x+Documentation

5. O software é baseado na comunidade DSpace. Mais informações em:

   http://www.dspace.org/why-use

6. Informação sobre o Hardware instalado:

   O RCAAP possui uma infraestrutura com uma vertente muito forte na virtualização assente no seguinte diagrama:



   O sistema de virtualização que suporta as máquinas virtuais do RCAAP é baseado na solução CITRIX XenServer que implementa uma solução de virtualização de classe empresarial comprovada, que oferece todos os recursos críticos necessários para qualquer implementação e virtualização de servidores. Focalizado na continuidade do negócio o serviço de virtualização gerido pelo grupo de Sistemas da FCT|FCCN implementa uma arquitetura geograficamente redundante (sala técnicas; SE03 e GRID) constituída por dois Clusters de virtualização autónomos, sem pontos singulares de falha inter-clusters. A interoperabilidade entre os dois Clusters estabelece um plano de recuperação de desastre (DRP- disaster recovery plan) que garante a continuidade do serviço em caso de indisponibilidade parcial ou total de um dos datacenters, com níveis base de RTO (Recovery time objective) máximo de 6 horas e RPO (Recovery point objective) de 24horas.

XVI. Security

R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.

Guidance:

The repository should analyze potential threats, assess risks, and create a consistent security system. It should describe damage scenarios based on malicious actions, human error, or technical failure that pose a threat to the repository and its data, products, services, and users. It should measure the likelihood and impact of such scenarios, decide which risk levels are acceptable, and determine which measures should be taken to counter the threats to the repository and its Designated Community. This should be an ongoing process.

For this Requirement, please describe:

● Procedures and arrangements in place to provide swift recovery or backup of essential services in the event of an outage.

● Your IT security system, disaster plan, and business continuity plan; employees with roles related to security (e.g., security officers); and any risk analysis tools (e.g., DRAMBORA) you use. This Requirement describes some of the aspects generally covered by others—for example, R12 (Workflows)—and is supplementary to R9 (Documented storage procedures).

Self-assessment statement:

O repositório realizou um processo de compatibilização da sua atuação com a ISO 16363 em 2015. Neste processo, o Serviço de Alojamento Repositório de Dados Científicos não fez parte. No entanto, por partilhar de meios e infraestruturas comuns, beneficiou do trabalho desenvolvido.

1. Lista de processos instalados e processos críticos:

   No âmbito do RCAAP foram identificados como processos críticos, aqueles que têm impacto direto:
   - No cumprimento das obrigações do contrato estabelecido com as ENTIDADES ADERENTES
   - No cumprimento da lei

   Identificação dos processos:

ID	Process Name	Process Description	Inputs	Outputs
P0	Manutenção serviço	Processo relacionado com a disponibilização do serviço	▪ Setup e update dos certificados digitais ▪ Setup dos Handles ▪ Setup e atualização dos serviços ▪ Setup da monitorização ▪ Agregação Portal ▪ Aplicação de testes	▪ Relatórios de Progresso ▪ Gestão de capacidade ▪ Problemas e soluções frequentes
P1	Preservação de conteúdos	Processo relacionado preservação dos conteúdos depositados nos serviços alojados	▪ Gestão de Processos ▪ Gestão de Riscos ▪ Processo de depósito de conteúdos	▪ Backups ▪ Export AIP
P2	Depósito de conteúdos	Processo de depósito de conteúdos nos serviços alojados	▪ Auto-depósito ▪ Configuração workflows ▪ Criação estrutura (Comunidades/Coleções)	▪ Produção científica ▪ Processo de Preservação de conteúdos
P3	Suporte (Helpdesk)	Processo de suporte de ocorrências	▪ Configurações de email RCAAP ▪ Configurações OTRS	▪ Métricas de desempenho ▪ Inquérito de satisfação
P4	Cessação do serviço	Processo de cessação do serviço RCAAP	▪ Plano de sucessão ▪ Plano de contigência	▪ Disponibilização dos dados e metadados
P5	Gestão de riscos	Processo de gestão de riscos do serviço RCAAP	▪ Inventário de activos (Hardware, Software, Recursos Humanos,..) ▪ Análise de risco	▪ Plano de tratamento do risco ▪ Plano de contigência

   Matriz:

		Utilizador	Gestor Repositório	Técnico RCAAP	Gestor RCAAP	Direção RCAAP
P0 - Manutenção serviço		I	R	A	A	
P1 - Preservação de conteúdos		C	R	I	A	
P2 - Depósito de conteúdos	R	C				
P3 - Suporte		R	C	I	A	
P4 - Cessação		I	C	C	R	
P5 - Gestão de riscos			I	R	C	

Legenda:

Responsible:	Pessoa que opera na atividade
Accountable:	Pessoa com poder de decisão
Consult:	Pessoa que deve ser incluída na operação ou na decisão
Inform:	Pessoa que necessita ser informada da ação ou decisão

Análise do impacto – relação entre o tempo passado e o nível de impacto causado pela inexistência do processo. Deste modo é definido o nível de criticidade do processo:

	0-1H	1-7H	7-24H	24H-30D	+ 30D
High					P1 P4
Medium				P0	
Low		P2		P3	P5

Análise dos riscos:

A análise dos riscos resultou de um trabalho efetuado em parceria com o projeto TIMBUS (Timeless Business Processes and Services - http://timbusproject.net/). Foi feito o levantamento do modelo contextual, em que são representadas as dependências no sistema, quer ao nível de Infraestrutura, Software e Sistema Operativo, modelo de Dados, Obrigações, e depois de definidos os requisitos, foi elaborado um modelo de Riscos, que tenham propensão para afetar o sistema, de forma a promover a preservação no RCAAP.

A metodologia usada pressupõe as seguintes fases:

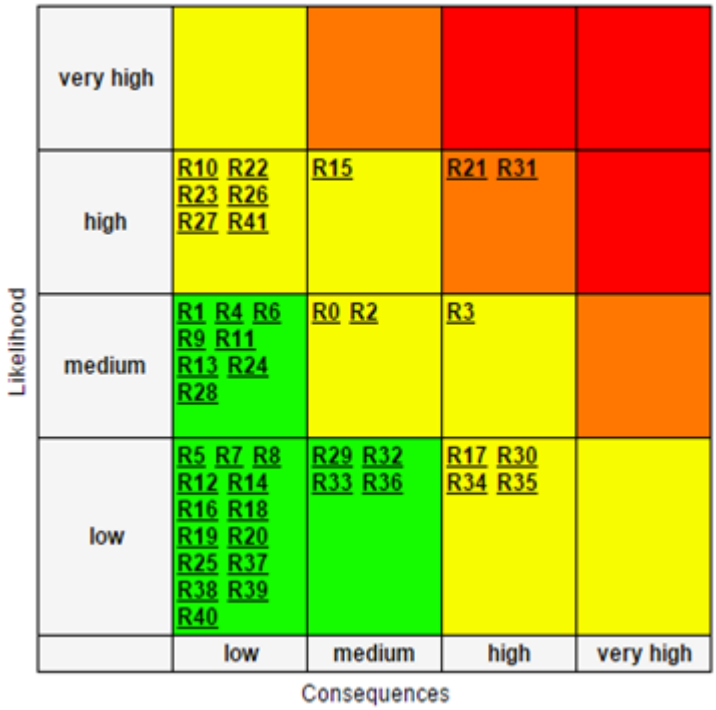
- Identificação do Risco
- Análise do risco
- Avaliação do risco

Com base no trabalho feito em parceira com o projeto TIMBUS. Neste modelo são definidos:

- Quais os elementos usados para aferir o risco
- Metadados para caracterizar os elementos do modelo

Avaliação dos Riscos

A figura mostra a matriz de riscos após a aplicação das estratégias de mitigação apontadas no projeto TIMBUS (controlos):



A identificação dos riscos pode ser consultada no anexo 1 deste documento.

2. Plano de contingência definido:

   O "Plano de Contingência" pretende antecipar e gerir o impacto duma eventual situação de catástrofe com os serviços RCAAP. De acordo com a ISO 16363 - 5.2.4 – o repositório deve possuir um plano de contingência que inclua pelo menos uma cópia de toda a informação digital numa localização geograficamente distante (incluindo uma cópia do plano de contingência).

   Nesse sentido foram elaborados cenários de recuperação baseados em 4 cenários:
   - C1 – Indisponibilidade do HOST
   - C2 – Perda permanente do HOST
   - C3 – Indisponibilidade de Backup
   - C4 – Violação de integridade no AIP (Archive Informational Package)

   Para cada um dos cenários existem instruções específicas e planos de ação para repor os serviços.

   Existem ainda um conjunto de procedimentos de operação relacionados com as seguintes tipologias:

   - Manutenção dos serviços
   - Backups e preservação dos conteúdos
   - Depósito de conteúdos
   - Suporte à comunidade
   - Gestão de riscos

ANEXO 1 – IDENTIFICAÇÂO DOS RISCOS

ID	Risk Name	Consequence	Event	Risk Asset
R0	Change of business model due to financial loss	high	E10	RCAAP Organization
R1	Changes in organizational structure due to change of business model	medium	E1	RCAAP Organization
R2	Changes in service due to change of business model	medium	E1	RCAAP Functionality
R3	Financial loss due to change of business model	high	E1	RCAAP Organization
R4	Functionality fault due to financial loss	medium	E10	RCAAP Functionality
R5	Functionality fault due to hardware unavailability*	medium	E12	RCAAP Functionality
R6	Functionality faults due to accidental system failure*	medium	E0	RCAAP Functionality
R7	Functionality faults due to changes in service	medium	E3	RCAAP Functionality
R8	Functionality faults due to changes to the data model	medium	E4	RCAAP Functionality
R9	Functionality faults due to environment changes	medium	E27	RCAAP Functionality
R10	Functionality faults due to internal or external attacks	medium	E13	RCAAP Functionality
R11	Functionality faults due to loss of expert knowledge	medium	E17	RCAAP Functionality
R12	Functionality faults due to software unavailability	medium	E20	RCAAP Functionality
R13	Functionality faults due to system changes*	medium	E23	RCAAP Functionality
R14	Functionality faults due to unavailability of core utilities*	medium	E24	RCAAP Functionality
R15	Functionality unavailability due to functionality fault	medium	E11	RCAAP Functionality
R16	Hardware unavailability due to local environmental phenomenon*	medium	E15	RCAAP Hardware
R17	Legal liability due to non-compliance with terms of contract due to deliberate system failure caused by FCCN	high	E5	RCAAP Organization
R18	Legal liability due to non-compliance with terms of contract due to failure to comply with FCCN obligations	high	E6	RCAAP Organization
R19	Legal liability due to non-compliance with terms of contract due to failure to provide data up until 30 days after the termination of the contract	high	E7	RCAAP Organization
R20	Legal liability due to non-compliance with terms of contract due to non-satisfaction of adhering entity rights	high	E9	RCAAP Organization
R21	Loss of data authenticity due to internal or external attacks	very high	E13	RCAAP Data
R22	Loss of data due to internal or external attacks	very high	E13	RCAAP Data
R23	Loss of data due to software dependency faults	very high	E21	RCAAP Data
R24	Loss of data integrity due to accidental system failure*	very high	E0	RCAAP Data
R25	Loss of data integrity due to changes to the data model	very high	E4	RCAAP Data
R26	Loss of data integrity due to internal or external attacks	very high	E13	RCAAP Data
R27	Loss of data integrity due to software faults	very high	E21	RCAAP Data
R28	Loss of expert knowledge due to changes in organizational structure	medium	E2	RCAAP Organization
R29	Loss or lack of metadata due to non-provision by the user	medium	E26	RCAAP Data
R30	Reputation Loss due to illicit activities	high	E25	RCAAP Organization
R31	Reputation Loss due to internal or external attacks	high	E13	RCAAP Organization
R32	Reputation Loss due to legal liability	high	E14	RCAAP Organization
R33	Reputation Loss due to loss of data	high	E16	RCAAP Organization
R34	Reputation Loss due to non-termination of contract with adhering entity	high	E19	RCAAP Organization
R35	Reputation loss due to failure to remove illegal content	high	E8	RCAAP Organization
R36	Reputation loss due to loss or lack of metadata	high	E18	RCAAP Organization
R37	Shortcomings in semantic understandability due to changes in data model	medium	E4	RCAAP Data
R38	Shortcomings in semantic understandability due to loss or lack of metadata	medium	E18	RCAAP Data
R39	Software faults due to software obsolescence*	medium	E22	RCAAP Software
R40	Software unavailability due to hardware unavailability*	medium	E12	RCAAP Software
R41	Software unavailability due to software faults	medium	E21	RCAAP Software

ANEXO 2