

# **Política de Gestão da Informação**

## **FCNAUP**

Proposta em desenvolvimento - v0

## Sumário

|                                                      |           |
|------------------------------------------------------|-----------|
| <b>Considerações iniciais .....</b>                  | <b>4</b>  |
| <b>1. Política de Gestão da Informação .....</b>     | <b>5</b>  |
| 1.1. Aos colaboradores .....                         | 5         |
| 1.2. Propósito e Objetivos .....                     | 5         |
| 1.3. Siglas Utilizadas .....                         | 6         |
| 1.4. Período de Validade .....                       | 6         |
| 1.5. Atores e Responsabilidades .....                | 6         |
| 1.5.1. Atores .....                                  | 6         |
| 1.5.2. Responsabilidades .....                       | 7         |
| 1.6. A Gestão da Informação .....                    | 7         |
| 1.7. Aplicação do MGSIU-AP .....                     | 8         |
| 1.7.1. Os processos .....                            | 8         |
| 1.7.2. Os serviços .....                             | 10        |
| 1.8. Segurança da informação .....                   | 12        |
| 1.8.1. Confidencialidade .....                       | 13        |
| 1.8.2. Integridade .....                             | 13        |
| 1.8.3. Disponibilidade .....                         | 14        |
| 1.8.4. Autenticidade .....                           | 14        |
| 1.8.5. Não-repúdio .....                             | 14        |
| 1.8.6. Legalidade .....                              | 15        |
| 1.8.7. Gestão de Risco .....                         | 15        |
| 1.8.8. Gestão de segurança e Melhoria Contínua ..... | 16        |
| 1.9. Formação .....                                  | 16        |
| 1.10. Supervisão e Auditoria .....                   | 16        |
| <b>2. Considerações Finais .....</b>                 | <b>17</b> |
| <b>3. Legislação e Normas .....</b>                  | <b>17</b> |
| 3.1. Legislação .....                                | 17        |

|                                           |           |
|-------------------------------------------|-----------|
| <b>3.2. Normas.....</b>                   | <b>19</b> |
| <b>4. Referências Bibliográficas.....</b> | <b>22</b> |

## **Considerações iniciais**

A presente proposta de Política de Gestão da Informação tem como objetivo clarificar os conteúdos necessários à Gestão da Informação e estabelecer as diretrizes para a implementação de um modelo de gestão da informação na FCNAUP.

A gestão da informação “consiste no estudo, conceção, implementação e desenvolvimento dos processos e serviços inerentes ao fluxo infocomunicacional, permitindo a construção de modelos de operacionalização de máxima eficiência e rentabilização” (PINTO, 2015:547).

A gestão da informação presume a atribuição de competências e encargos que devem ser analisados sistematicamente, depois de revisão de todos os procedimentos de trabalho, juntamente com os colaboradores responsáveis pelos processos.

Nesta política serão apresentados os propósitos e objetivos da mesma, quais os atores e as suas responsabilidades, bem como as tarefas associadas à gestão da informação.

Em seguida, será exposto um modelo de gestão da informação adaptado ao ambiente universitário, bem como diretrizes básicas no âmbito da Preservação e segurança da informação e as respetivas considerações finais.

## **1. Política de Gestão da Informação**

### **1.1. Aos colaboradores**

Serve a presente política para o estabelecimento das diretrizes da política de gestão da informação a ser aplicada na FCNAUP, de modo a promover a identificação, aquisição, organização, armazenamento e disseminação de informação e conhecimento.

Deve ser levada em consideração todas as normas existentes que permitam a organização e o tratamento da informação, bem como a segurança da mesma.

O desconhecimento da política de gestão da informação por parte dos colaboradores da FCNAUP, não invalida o não cumprimento das diretrizes abaixo descritas.

Nesse sentido, solicita-se atenção à presente política.

### **1.2. Propósito e Objetivos**

A política de gestão da informação tem como principal objetivo dar um conjunto de recomendações e de critérios utilizados ou a ser utilizados pela FCNAUP.

Por conseguinte, são apresentadas todas as atividades da gestão da informação, a aplicação do MGSIU-AP na FCNAUP e os critérios de segurança da informação, para uma melhor integridade, confidencialidade e disponibilidade da informação.

A presente política aplica-se a informação nos mais diversos formatos.

### **1.3. Siglas Utilizadas**

|                 |                                                                                 |
|-----------------|---------------------------------------------------------------------------------|
| <b>FCNAUP</b>   | Faculdade de Nutrição e Alimentação da<br>Universidade do Porto                 |
| <b>SDI</b>      | Serviço de Documentação e Informação                                            |
| <b>U.Porto</b>  | Universidade do Porto                                                           |
| <b>MGSIU-AP</b> | Modelo de Gestão de Sistema de Informação<br>Universitário – Ativa e Permanente |
| <b>SI-AP</b>    | Sistema de Informação – Ativa e Permanente                                      |
| <b>GI</b>       | Gestão da Informação                                                            |
| <b>UE</b>       | União Europeia                                                                  |

### **1.4. Período de Validade**

A política de gestão da informação entrará em vigor no dia seguinte à sua aprovação.

A presente política é válida até à sua revogação ou substituição por uma nova versão, tendo o SDI a responsabilidade de propor melhorias à política que poderão dar origem a outra versão da mesma.

### **1.5. Atores e Responsabilidades**

#### **1.5.1. Atores**

Os atores envolvidos na presente política são os seguintes:

- O diretor da FCNAUP;

- O responsável pelo SDI;
- Os colaboradores da FCNAUP.

### **1.5.2. Responsabilidades**

As responsabilidades aqui enumeradas são relativas aos atores em cima referenciados:

- I. O diretor da FCNAUP deve aprovar a política, bem como apoiar ao cumprimento da mesma.
- II. O responsável pelo SDI deve aplicar e garantir que a política de gestão da informação é conhecida, para que se cumpram todos os critérios da gestão da informação, as boas práticas da segurança da informação e a aplicação do MGSIU-AP na FCNAUP.
- III. Os colaboradores da FCNAUP devem aplicar e cumprir com as diretrizes expostas na presente política.

### **1.6. A Gestão da Informação**

A gestão da informação é caracterizada por um conjunto de processos que permite que as organizações se adaptem aos diversos ambientes internos e externos de acordo com as atividades de aprendizagem organizacional (*Choo*, 2003). Já para Rascão (2006) a gestão da informação encontra-se relacionada com a forma como percebemos a informação e por isso a gestão da informação tem em conta todas as atividades das organizações e como estas disseminam a informação para ajudar às tomadas da decisão.

Embora existam vários modelos da gestão da informação todos são consensuais em relação a certas etapas da gestão da informação: a aquisição, o tratamento, a distribuição e a utilização da informação.

Alguns dos modelos de gestão da informação são o modelo de *Mcgee* e *Prusak* (1994), um modelo de 7 etapas que se foca no tratamento da informação, o modelo de *Davenport* (1998) que apresenta quatro etapas ligadas à obtenção da informação e o modelo de *Choo* (2003) onde se realça a

identificação das necessidades de informação, a organização da informação e o comportamento adaptativo.

Estes modelos carecem, contudo, de uma clara assunção da produção informacional, a par da organização e representação da informação e do comportamento informacional, do foco no fluxo infocomunicacional e de uma GI assumida na perspectiva CI como área transversal e aplicada, que se espelha no modelo que se descreve de seguida.

### **1.7. Aplicação do MGSIU-AP**

O Modelo de Gestão do Sistema de Informação Universitário - Ativa e Permanente (MGSIU-AP) (Pinto, 2015) é centrado no fluxo infocomunicacional e tendo em vista a criação do SIU-AP, isto é, o Sistema de Informação Universitário - Ativa e Permanente (Pinto e Silva, 2005). Este modelo é composto por três componentes sistémicos – o Institucional e de Gestão Organizacional, o Infocomunicacional e o Tecnológico – e um conjunto de seis processos e onze serviços em GI.

O MGSIU-AP é aplicado na FCNAUP a partir do conjunto de processos e serviços existentes na componente de informação. Em seguida são explicitado os processos e os serviços que já foram aplicados na FCNAUP e aqueles que terão ser implementados.

#### **1.7.1. Os processos**

*Tabela 1 - Processos do modelo MGSIU-AP*

| <b>Processos (Pinto 2015)</b>                              | <b>Como implementar na FCNAUP</b>                                                                                                                                            |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Análise e alinhamento institucional e organizacional da GI | Este processo pode ser obtido através da análise orgânico-funcional, da avaliação das necessidades informacionais da organização e da definição de uma política de Gestão da |

| <b>Processos (Pinto 2015)</b>                                                                                    | <b>Como implementar na FCNAUP</b>                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                  | Informação e Tecnologias de Informação e consequentes planos (incluindo Plano de Preservação e Segurança da Informação), alinhados com a estratégia e política da FCNAUP                                                                                                        |
| Conceção, implementação e manutenção de plataformas                                                              | Este processo pode ser implementado com a especificação de requisitos, criação de perfis de utilizadores e grupos de sistemas tecnológicos implementados, bem como a criação e normalização de procedimentos.                                                                   |
| Produção/Criação informacional transaccional (e interação com o SI-AP)                                           | Este processo será obtido a partir da abordagem integrada da digitalização, captura e extração bem como produção nado-digital, gestão de correspondência (tradicional e email), produção informacional SIGARRA e sistemas conexos, etc.                                         |
| Processamento e avaliação informacional (transaccional e na relação transaccional/SI-AP)                         | O processamento convoca diversos serviços, nomeadamente o de gestão de meta-informação ou o de avaliação, seleção e determinação do destino final da informação (efetuada a partir do recenseamento e consequente identificação de séries informacionais e respetivo produtor). |
| Armazenamento e preservação, com a integração e manutenção no SI-AP, como evidência, memória e fonte estratégica | Este processo deve ser obtido a partir da incorporação/ingestão da informação (analógica e digital); recenseamento das unidades físicas, digitalização e transferências                                                                                                         |

| <b>Processos (Pinto 2015)</b> | <b>Como implementar na FCNAUP</b>                                                                                                                                                                                                                                                                                     |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | de suporte; gestão do repositório digital, gestão da preservação.                                                                                                                                                                                                                                                     |
| Comunicação e uso do SI-AP    | Este processo é obtido através das plataformas que disponibilizam meta-informação e informação (FCNAUP, U.PORTO, recursos externos, etc.), permitindo a sua disseminação, pesquisa e recuperação, bem como a publicação de conteúdos, comunicação da produção científica e exportação e importação de metainformação. |

### 1.7.2. Os serviços

*Tabela 2 - Serviços do MGSIU-AP*

| <b>Serviço (Pinto, 2015)</b>                                                        | <b>Como implementar na FCNAUP</b>                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S1. Gestão de perfis, grupos e utilizadores                                         | Este serviço encontra-se parcialmente implementado nas plataformas existentes devendo responder a novas necessidades e requisitos de interoperação entre sistemas.                                                                                                   |
| S2. Análise de negócio, especificação e gestão de processos e fluxos informacionais | Este serviço é obtido a partir do mapeamento e modelação de fluxos de informação.                                                                                                                                                                                    |
| S3. Estruturação e gestão da metainformação                                         | .Este serviço envolve a gestão do controlo de autoridade, a classificação, descrição e criação de pontos de acessos, a criação de meta-informação técnica e estrutural (associadas por exemplo a objetos digitais), relacionando-se com o controlo de autoridade e a |

| <b>Serviço (Pinto, 2015)</b>                                                             | <b>Como implementar na FCNAUP</b>                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                          | existência de listas de termos, listas de tipologias de documentos e gestão do Plano de Classificação.                                                                                                                                                                      |
| S4. Gestão da propriedade intelectual e outros direitos                                  | Este serviço deve ser implementado a partir da criação de uma política de propriedade intelectual, para possível definição de regras formalizadas a cumprir.                                                                                                                |
| S5. Digitalização e registo de documentos                                                | Este serviço será implementado a partir da análise orgânico-funcional, do mapeamento de processos, da identificação da produção informacional e consequente implementação do sistema de gestão de correspondência, gestão de arquivo e outros sistemas já em funcionamento. |
| S6. Avaliação, seleção, retenção e eliminação da informação                              | Este serviço deve ser implementado a partir do recenseamento e identificação de séries informacionais com a avaliação, seleção, retenção e eliminação da informação, aplicando a abordagem sistémica e a metodologia desenvolvida na U.Porto.                               |
| S7. Armazenamento, alojamento e repositórios (incorporação/depósito/in gestão e arquivo) | Este serviço deve ser implementado a partir do recenseamento e armazenamento físico e digital de informação administrativa, produção científica e técnica, publicações eletrónicas e gestão de outros recursos informacionais detidos pela U.Porto.                         |
| S8. Disseminação, pesquisa e recuperação/busca de informação                             | Este serviço é obtido a partir dos serviços de informação e, sistemas tecnológicos de informação implementados a nível da FCNAUP, da U.Porto e outras plataformas externas.                                                                                                 |
| S9. Exportação, importação e recolha de metainformação e informação                      | Este serviço é obtido a partir dos sistemas tecnológicos de informação implementados a nível da U.Porto.                                                                                                                                                                    |
| S10. Comunicação da ciência/publicação                                                   | Este serviço encontra-se ativo na U.Porto o SIGARRA, o Repositório da U.Porto, os serviços de Edições, as plataformas de                                                                                                                                                    |

| <b>Serviço (Pinto, 2015)</b> | <b>Como implementar na FCNAUP</b>                                                                                                                                                                                                                                                                                  |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | alojamento e gestão de conferências e revistas científicas em acesso aberto, etc.                                                                                                                                                                                                                                  |
| S11. Preservação e segurança | Este serviço deve estar alinhado com a estratégia da FCNAUP, a partir da criação da Políticas de Gestão da Informação e Tecnologias da Informação, consequente Política e Plano de Preservação e Segurança da Informação (física e digital) e inerente sistema de gestão da preservação já adquirido pela U.Porto. |

### **1.8.Segurança da informação**

A Segurança da Informação deverá ser assumida em articulação com a Preservação da Informação. Encontra-se integrada nesta política, para que todas as operações da FCNAUP possam funcionar, mesmo em situações de urgência e para que deste modo sejam assegurados e ativados todos os planos e os procedimentos de *backup* dos sistemas de informação desta instituição.

Os pontos mais fundamentais da segurança da informação são a confidencialidade, a integridade e a disponibilidade, no entanto, são ainda abordados mais conceitos nesta política para uma maior abrangência e proteção da informação.

A FCNAUP deve assim assegurar as boas práticas da segurança da informação a partir dos seguintes objetivos:

1. Assegurar a conformidade das leis e regulamentos existentes;
2. Cumprir com as tarefas da segurança da informação enumeradas na política de gestão da informação;
3. Estabelecer controlos para proteger da melhor maneira a sua informação contra acessos não autorizados;

4. Assegurar a proteção dos dados pessoais, de acordo com o Regulamento de proteção de dados pessoais da Universidade do Porto;
5. Assegurar que todos os serviços orgânicos da FCNAUP continuam a funcionar na sua plenitude independentemente de qualquer risco de segurança;
6. Certificar que todos os fornecedores da FCNAUP estão de acordo com os requerimentos da segurança da informação enumerados na presente política.

#### **1.8.1. Confidencialidade**

A confidencialidade tem como objetivo restringir a informação acedida, permitindo que apenas as pessoas que têm direito a aceder a essa informação, tenham acesso à mesma.

As quebras de confidencialidade podem ocorrer de diversas maneiras e podem ser por vezes realizadas intencionalmente. Algumas das situações onde pode ocorrer quebra de confidencialidade é a de conceder informação confidencial por vias não protegidas, como no *email*, ou por telefone, ou se essa informação tenha sido roubada.

#### **1.8.2. Integridade**

A integridade garante que os dados que estão a ser acedidos não foram alterados em nenhum momento por colaboradores não autorizados a esse fim. Ou seja, apenas as pessoas autorizadas, podem alterar ou até destruir dados e informação.

A integridade deve andar sempre de mãos dadas com a confidencialidade e por isso a quebra de confidencialidade, pode significar a perda de integridade e vice-versa.

### **1.8.3. Disponibilidade**

A disponibilidade significa que a informação deve estar disponível aos colaboradores sempre que necessário e por isso todos os sistemas de informação e todos os canais de comunicação da FCNAUP devem operar corretamente.

### **1.8.4. Autenticidade**

A autenticidade significa que a informação que estamos a aceder é completamente genuína. Existem várias formas de garantir a autenticidade, sendo que uma delas é a autenticação por credenciais nos sistemas de informação, sendo esta autenticação constituída por um nome de utilizador e por uma palavra-passe.

No entanto, a autenticidade também pode ser garantida através da utilização da assinatura digital, uma vez que esta garante por quem foi elaborado o documento, a data e a hora, sendo impossível de alterar essa informação. Em documentos confidenciais é assim recomendada a utilização da assinatura digital.

### **1.8.5. Não-repúdio**

O não-repúdio significa que todos os colaboradores devem assumir as responsabilidades do seu contrato de trabalho e não podem negar o seu envolvimento em ações que estes mesmos realizaram, mesmo que essas ações levem a consequências para a segurança da informação.

### **1.8.6. Legalidade**

A legalidade significa que a FCNAUP devem garantir a segurança da informação de acordo com a legislação existente.

Um dos regulamentos que permitem a segurança da informação é o Regulamento de Execução (UE) 2018/151 de 30 de janeiro de 2018 que aborda a especificação dos elementos a ter em conta pelos prestadores de serviços digitais na gestão de riscos que se colocam à segurança das redes e dos sistemas de informação. Outra legislação a cumprir é o regulamento (UE) 2016/679 relativo à proteção dos dados pessoais.

A FCNAUP deve deste modo assegurar a segurança da informação dos colaboradores, dos seus estudantes e de outros utilizadores externos de acordo com a legislação atual.

### **1.8.7. Gestão de Risco**

A gestão de riscos permite que as organizações possam minimizar as suas perdas e maximizar as suas oportunidades, a partir de uma constante análise, avaliação e monitorização das atividades e dos processos existentes na FCNAUP.

Para uma efetiva gestão de riscos, deve ser criada uma lista com os riscos positivos e os riscos negativos, devendo ser considerada todas as causas e consequências dos mesmos. A identificação dos riscos pode levar à criação de vantagens competitivas para a organização, mas também à prevenção dos riscos negativos.

A prevenção dos riscos é primordial para a recuperação de desastres, por isso, todas as vulnerabilidades e falhas dos sistemas da FCNAUP devem ser identificadas e analisadas.

### **1.8.8. Gestão de segurança e Melhoria Contínua**

A gestão da segurança da informação requiere que haja uma contínua análise e avaliação da segurança na FCNAUP para perceber se todos os critérios da gestão da informação acima enumerados são cumpridos.

Para a possível melhoria contínua é necessário que a segurança da informação e o controlo seja assegurado em todos os sistemas de informação da FCNAUP, bem como se cumpram todos os aspetos jurídicos publicados no Diário da República.

A partir da gestão de segurança e da melhoria contínua é possível identificar certos problemas de controlo e garantir que estes problemas não surjam mais tarde. Esta gestão da segurança e melhoria contínua pode ser explorada na FCNAUP a partir de envio de inquéritos aos utilizadores para possíveis sugestões de melhoria e também até por possíveis ações de formação para conscientização de utilizadores internos e externos.

### **1.9. Formação**

Caso necessário a entidade criadora desta política deverá dar formação aos colaboradores da FCNAUP, para estes fiquem devidamente informados da mesma.

### **1.10. Supervisão e Auditoria**

A política de gestão da informação deve sofrer auditorias com uma periodicidade de cinco anos, devendo ser alvo de mudanças sempre que necessário.

As mudanças da política de gestão da informação ficam a cargo do responsável do SDI e devem ser aprovadas por todos os colaboradores da FCNAUP.

## **2. Considerações Finais**

Espera-se que esta política sirva como um instrumento de trabalho para todos os colaboradores da FCNAUP, bem como para aqueles que integrarem esta instituição.

A implementação de novos sistemas de informação pressupõem que estes devem adotar metodologias corretas e de acordo com as necessidades informacionais das organizações, por isso, a política de gestão da informação torna-se essencial como um guia para a correta implementação destes sistemas.

Esta política deve ter uma intervenção ao longo do tempo e por isso, o SDI fica à responsabilidade de a modificar e melhorar sempre que assim o for necessário e exigido.

## **3. Legislação e Normas**

### **3.1. Legislação**

#### **A. Decreto-Lei nº 290-d/1999, de 2 de agosto**

- Aprova o regime jurídico dos documentos eletrónicos e da assinatura digital.

#### **B. Lei nº 46/2007, de 24 de agosto**

- Regula o acesso aos documentos administrativos e a sua reutilização.

C. Decreto-Lei n.º 88/2009 de 09 de abril

- Procede à quarta alteração ao Decreto-Lei n.º 290-D/99, de 2 de agosto, que estabelece o regime jurídico dos documentos eletrónicos e da assinatura digital, e à primeira alteração ao Decreto-Lei n.º 116-A/2006, de 16 de junho, que cria o Sistema de Certificação Eletrónica do Estado.

D. Decreto-Lei n.º 47/2004 de 03 de março

- Define o regime geral das incorporações da documentação de valor permanente em arquivos públicos.

E. Decreto-Lei nº16/1993 de 23 janeiro

- Aprova o regime geral dos arquivos e do património arquivístico, visando definir os princípios que devem presidir a sua organização, inventariação, classificação e conservação, bem como as operações que permitem a sua guarda, acesso e uso, e a punição de atos de destruição, alienação, exportação ou ocultação.

F. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016

- Regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

### 3.2. Normas

#### A. Norma ISAAR

- Esta norma dá diretivas para a organização de registos de autoridade arquivística que forneçam descrições de entidades relacionadas à produção e manutenção de arquivos.

#### B. Norma ISAD

- Esta norma estabelece orientações gerais para a descrição arquivística.

#### C. Norma ISO 30300/2011

- Norma introdutória de sistema de gestão para documentos de arquivo, abordando os vocabulários e as terminologias.

#### D. Norma ISO 30301/2011

- Norma que estabelece os requisitos para a implementação do sistema de gestão de documentos de arquivo.

#### E. Norma 4041-2/2005

- Esta norma estabelece os princípios diretores na gestão de documentos de arquivo.

F. Norma ISO 18492/2005

- Esta norma fornece uma orientação metodológica para a preservação e recuperação a longo prazo de informações de documentos eletrónicos autênticos, quando o período de retenção excede a vida esperada da tecnologia, que é o suporte dessa mesma informação.

G. Norma IEC 82045-1:2008

- Esta norma apresenta um conjunto de métodos e princípios para a gestão de documentos.

H. Norma Portuguesa EN ISO 11442: 2014

- Esta norma explicita um conjunto de regras para a gestão de uma tipologia de documentos – os documentos técnicos.

I. Norma ISO 15801:2004

- Esta norma explica como implementar sistemas de gestão de documentos e de como gerir a segurança da informação destes sistemas.

J. Norma ISO/TR 18492:2005

- Esta norma explica como preservar documentos eletrónicos a longo-prazo.

K. Norma ISO 13028:2010

- Esta norma elucida sobre os benefícios e os riscos de se digitalizar os documentos, bem como as melhores práticas de digitalizar, para implementar estes documentos nos sistemas.

L. Norma Portuguesa 4438-1

- Esta norma explica os princípios e métodos da gestão de arquivos.

M. Norma Portuguesa 4438-2

- Esta norma explica como implementar políticas de gestão de arquivo e responsabilidades.

N. Norma Portuguesa ISO 11799:2014

- Esta norma elucida das melhores características que os depósitos físicos de arquivo e biblioteca devem possuir.

O. Norma ISO/TS 23081

- Esta norma cobre todos os princípios sobre a gestão da metainformação dos documentos que podem ser aplicados a todos os documentos, aos processos que os afetam, aos sistemas e também à organização que é responsável pela sua gestão.

P. Norma ISO 14721:2003

- Esta norma aborda um conjunto de recomendações de boas práticas para a implementação de sistemas de arquivo e esclarece um conjunto de funções de preservação da informação no arquivo.

#### 4. Referências Bibliográficas

ANACOM (1999). *Decreto-Lei nº 290-D/99 de 2 de agosto*. Disponível em URL <<https://www.anacom.pt/render.jsp?contentId=957061&languageId=0>>

BANGOR (2015). *Information Security Policy*. Universidade de Prifysgol Bangor. 1-13. Disponível em URL <<https://www.bangor.ac.uk/planning/policy-register/documents/information-security-policy.pdf>>

Best, David P. (2010). The future of Information management. *Records Management Journal*. 20(1), 61-71. Disponível em URL <<https://doi.org/10.1108/09565691011039834>>

DIÁRIO DA REPÚBLICA ELETRÓNICO (1988). *Decreto-Lei nº447/88*. Disponível em URL <<https://dre.pt/pesquisa/-/search/356515/details/normal?jp=true/en/en/en>>

DIÁRIO DA REPÚBLICA ELETRÓNICO (1993). *Decreto-Lei nº16/93*. Disponível em URL <[https://dre.pt/web/guest/pesquisa/-/search/584777/details/normal?p\\_p\\_auth=mX3WsL0B](https://dre.pt/web/guest/pesquisa/-/search/584777/details/normal?p_p_auth=mX3WsL0B)>

DIÁRIO DA REPÚBLICA (2009). *Decreto-Lei nº88/2009 de 9 de abril*. Disponível em URL <[http://www.dgpj.mj.pt/sections/leis-da-justica/pdf-ult2/decreto-lei-n-88-2009-de/downloadFile/file/DL\\_88.2009.pdf?nocache=1239264486.31](http://www.dgpj.mj.pt/sections/leis-da-justica/pdf-ult2/decreto-lei-n-88-2009-de/downloadFile/file/DL_88.2009.pdf?nocache=1239264486.31)>

DIÁRIO DA REPÚBLICA (2004). *Decreto-Lei nº47/2004*. Disponível em URL <[http://www.adporto.pt/ficheiros\\_a\\_descarregar/DL\\_47\\_2004\\_Reg\\_G\\_Incorp.pdf](http://www.adporto.pt/ficheiros_a_descarregar/DL_47_2004_Reg_G_Incorp.pdf)>

HAWKINS, Steve M.; YEN, David C.; CHOU; David C. (2000). Disaster recovery planning: a strategy for data security. *Information Management & Computer Security*. Vol.8, nº5, 222-230. Disponível em URL <<http://dx.doi.org/10.1108/09685220010353150>>

Instituto Português da Qualidade (2014). *Documentação técnica de produtos*. 1-16.

Instituto Português da Qualidade (2008). *Gestão de documentos. Parte 1: Princípios e métodos*. 1-38.

Instituto Português da Qualidade (2005). *Gestão de documentos de arquivo: Parte 1: Princípios diretores*. 1-31.

Instituto Português da Qualidade (2005). *Gestão de documentos de arquivo: Parte 2: Recomendações de aplicação*. 1-58.

Instituto Português da Qualidade (2014). *Requisitos para armazenamento de materiais de arquivo*

*e biblioteca. 1-20.*

ISO. International Organization for Standardization (2003). ISO 14721:2003. *Space data and information transfer systems*. Open archival information system (OAIS). Reference model.

ISO. International Organization for Standardization (2005). ISO/TR 18492:2005. *Long-term preservation of electronic document- based information*.

ISO. International Organization for Standardization -ISO/TR 13028:2010. *-Information and documentation: Implementation guidelines for digitization of records*

ISO. International Organization for Standardization (2004) ISO/TR 15801:2004. *Electronic imaging : Information stored electronically : Recommendations for trustworthiness and reliability*.

ISO. International Organization for Standardization (2006). ISO/TS 23081:2006. *Information and documentation. Records management processes. Metadata for records (parte 1, 2 e 3)*

Pinto, M. M. (2015). *A Gestão da Informação nas Universidades Públicas Portuguesas: Reequacionamento e proposta de modelo*. (Tese de Doutoramento em Informação e Comunicação em Plataformas Digitais), Universidade do Porto - Universidade de Aveiro

PGDL (2007). *Lei nº46/2007 de 24 de agosto*. Disponível em URL [http://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=931&tabela=leis](http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=931&tabela=leis)>

UNIVERSIDAD DE MURCIA (2012). *Política de Seguridad de la Información*. Universidade de Múrcia, Múrcia. 1-16. Disponível em URL <<https://sede.um.es/sede/normativa/politica-de-seguridad-de-la-informacion/pdf/137.pdf>>