Julho – 2017

A gestão da informação com foco na mobilidade, colaboração e segurança: o caso de uma Associação Cultural

Fernando Ribeiro

Dissertação de Mestrado

Mestrado em Informação Empresarial

Versão Final

Julho – 2017

A gestão da informação
com foco na mobilidade, colaboração e segurança:
o caso de uma Associação Cultural

Fernando Ribeiro

Dissertação de Mestrado
apresentado ao Instituto de Contabilidade e Administração do Porto
para a obtenção do grau de Mestre em Informação Empresarial,
sob orientação da Prof. Doutora Ana Lúcia Terra

Julho – 2017

Resumo

A grande diversidade de dispositivos móveis e a crescente mobilidade dos utilizadores, num ambiente de trabalho colaborativo, coloca novos desafios para a gestão e segurança da informação. Este estudo analisa a forma como uma associação cultural implementou um sistema de gestão da informação baseado na nuvem. É descrita a problemática existente e a forma como a organização efetuou o levantamento de necessidades informacionais, definiu o plano de classificação e gestão da informação, instituiu um conjunto de regras e boas práticas a observar pelos colaboradores, implementou a plataforma colaborativa de gestão da informação na nuvem e conduziu a sua adoção pelos colaboradores. São detalhadas a funcionalidades oferecidas pela plataforma, a forma como os utilizadores foram formados na sua utilização e como essas funcionalidades foram assimiladas e integradas nas tarefas quotidianas desempenhadas pelos colaboradores. É feita uma análise crítica aos resultados da adoção do sistema de informação na perceção do valor da informação, nos processos de trabalho quotidianos, no trabalho colaborativo entre departamentos e com parceiros externos e no desempenho coletivo e individual.

Palavras-chave: gestão da informação, mobilidade, colaboração, segurança, computação na nuvem.

Abstract

The wide diversity of mobile devices and the increasing mobility of users, in a collaborative working environment, poses new challenges for information management and security. This study looks at how a cultural association has implemented a cloud-based information management system. It describes the existing problem and how the organization carried out the survey of information needs, defined the classification and information management plan, established a set of rules and good practices to be observed by employees, implemented the collaborative platform for information management in the cloud and led to its adoption by its employees. The functionalities offered by the platform are described, as also how users were trained in their use and how these functionalities were assimilated and integrated into the daily tasks performed by employees. A critical analysis is made of the results of adopting the information system in the perception of the value of information, in the daily work processes, in the collaborative work between departments and with external partners and in the collective and individual performance.

Keywords: information management, mobility, collaboration, security, cloud computing.

Agradecimentos

À Doutora Ana Terra, pela sua orientação e apoio, pela sua disponibilidade e simpatia, pelo seu rigor e exigência e, acima de tudo, pelos conhecimentos partilhados.

À ESEIG, ao ISCAP e a todos os seus professores que me contagiaram com os seus conhecimentos e que me fizeram sentir privilegiado por isso.

A todos os Acertinos, construtores de utopias e amigos de sempre, que desde a primeira hora abraçaram e apoiaram esta ideia.

Ao meu pai, Luís, rochedo inabalável e exemplo de retidão, que sempre me ensinou que eu podia fazer o que quisesse, desde que o fizesse bem.

À minha mãe, Amélia, a estrelinha mais brilhante de todo o firmamento e sempre presente no meu coração, que me ensinou a ver o lado mais bonito de tudo.

À Alexandra, companheira de vida e de aventuras que, com o seu entusiasmo e força de vontade, me faz acreditar que tudo é possível.

Muito obrigado!

Lista de siglas e acrónimos

Neste documento são utilizadas siglas e acrónimos de designações comuns, apenas apresentados aquando da sua primeira utilização. As siglas e acrónimos utilizados são:

ACERT	Associação Cultural e Recreativa de Tondela
ADRL	Associação para o Desenvolvimento Rural de Lafões
ARPANET	Advanced Research Projects Agency Network
AWS	Amazon Web Services Amazon
BSI	British Standards Institution
CC	Cloud Computing
CRM	Costumer Relationship Manager
CVE	Common Vulnerabilities and Exposures
DARPA	Defense Advanced Research Projects Agency
EAP	European Academy of Participation
GCE	Google Compute Engine
HTML	Hypertext Markup Language
IaaS	Infrastructure as a Service

ICE	Instituto das Comunidades Educativas
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IPP	Instituto Politécnico do Porto
IRMT	International Records Management Trust
ISCAP	Instituto Superior de Contabilidade e Administração do Porto
ISCTE	Instituto Superior das Ciências do Trabalho e da Empresa
ISO	International Organization for Standardization
LLP	Lifelong Learning Programme
MIT	Massachusetts Institute of Technology
MMS	Multimedia Message Service
NIST	National Institute of Standards and Technology
Noark	Norsk arkivstandard (Norwegian Archive Standard)
PaaS	Platform as a Service
PDF	Portable Document Format
PSI	Política de Segurança da Informação
S3	Simple Storage Service
SaaS	Software as a Service
SMS	Short Message Service
SPI	SaaS, PaaS e IaaS
SSD	Solid State Drive
TCP/IP	Transmission Control Protocol/Internet Protocol
TIC	Tecnologias da Informação e Comunicação
VPS	Virtual Private Server

Índice geral

Índice de tabelas

Índice de figuras

1. Introdução

"Maya: Eu acho que a colónia [de férias] prova que o impossível é impossível.
Repórter: O impossível é impossível, queres explicar um bocadinho melhor?
Maya: É que, ao fim e ao cabo, consegue-se sempre arranjar uma solução, o impossível é só uma espécie de exagero para difícil."

– Excerto de uma entrevista a Maya Al-Kadri, 15 anos, invisual.
(Alves, Silva, Carvalho e Vieira, 2015)

Oralmente, à volta de uma fogueira, ou de forma escrita, sobre uma placa de barro, a necessidade de preservação da informação sempre foi uma preocupação que se confunde com a própria historia da humanidade. Esta necessidade reflete o reconhecimento da importância da informação para a compreensão, explicação e registo de fenómenos ou acontecimentos observados e para a explicitação de saberes, ideias e significados, traduzindo-se na criação de conhecimento. A informação torna-se um bem que importa controlar, preservar e transmitir de forma passível de ser utilizada estrategicamente no futuro e cujo valor é diretamente proporcional ao seu contributo para a resolução de problemas, para prever acontecimentos futuros e auxiliar a tomada de decisão, aportando vantagens competitivas às organizações, grupos sociais ou indivíduos seus detentores. No entanto, o crescente volume de informação constantemente produzido, representa um importante desafio para a sua preservação, motivando a utilização de técnicas cada vez mais complexas para o seu registo, organização, manutenção e recuperação.

A evolução do paradigma custodial para o paradigma pós custodial, nos finais do século XX, motivou importantes e profundas alterações na forma como a informação é entendida e gerida. A perspetiva do arquivo como depósito documental é suplantada pela noção de gestão e valorização da informação, o foco deixa de ser o documento em si e passa a ser o seu conteúdo informacional, à preservação dos registos para efeitos legais e históricos é acrescentada a necessidade de informação como suporte de decisão e maior eficácia administrativa e os utilizadores evoluem de meros consumidores passivos para adquirirem também um papel de produtores ativos de informação.

Atualmente, o ritmo a que se verificam as inovações tecnológicas, nomeadamente nas tecnologias da informação e comunicação, bem como as novas formas de trabalho, onde a colaboração e o nomadismo assumem um papel preponderante, se por um lado representam novas oportunidades para as organizações, por outro, colocam desafios acrescidos à gestão da informação. Como consequência, as organizações procuram soluções que lhes permitam gerir, de forma eficaz, o crescente volume de informação, e ao mesmo tempo, garantir a sua disponibilidade, em tempo útil e de forma segura, sem barreiras geográficas ou temporais, em diversas plataformas e formatos.

Numa associação cultural, com cerca de duas dezenas de colaboradores permanentes, um número variável de colaboradores pontuais e diversos parceiros externos, a informação gerada e adquirida é de extrema importância. No entanto, para ser útil, esta deve estar sempre disponível, atualizada e facilmente acessível. Por outro lado, as necessidades de

mobilidade dos seus colaboradores e os diversos dispositivos e plataformas utilizadas – computadores portáteis, *tablets* ou *smartphones* – representam um desafio acrescido, quer no que diz respeito ao acesso à informação, de forma atempada e em segurança, quer ao desenvolvimento de qualquer trabalho colaborativo.

Para responder a este desafio foi necessário, por um lado, a conceção de um plano de organização da informação, complementado com ações de sensibilização e formação dos colaboradores e, por outro lado, a criação de estruturas tecnológicas que permitiram o acesso e a partilha eficaz da informação, de modo a facilitar o trabalho colaborativo e garantir o acesso à informação a partir de diversas plataformas, em tempo real, sem constrangimentos geográficos ou temporais e de forma totalmente segura.

Esta dissertação está organizada em quatro capítulos, correspondendo o primeiro a esta introdução. No segundo capítulo, procedemos à revisão da literatura existente, de forma a estabelecer o estado da arte, e refletimos sobre a importância e o significado gestão da informação, bem como sobre os desafios e oportunidades que a evolução tecnológica e as formas de trabalho emergentes representam para a gestão e segurança da informação num contexto de grande mobilidade dos utilizadores. No terceiro capítulo, apresentamos o estudo de caso de uma associação cultural, onde caraterizamos a organização e damos conta das suas dificuldades na gestão da informação produzida e adquirida e, em sequência, analisamos a forma como está a ser implementado e usado um sistema de gestão da informação baseado na cloud, num contexto de trabalho colaborativo e de grande nomadicidade. No quarto capítulo, procedemos a uma análise critica e partilhamos as conclusões deste trabalho. No final desta dissertação, listamos as referências bibliográficas que lhe dão suporte e, em apêndice, os documentos criados para a instituição no âmbito deste estudo de caso.

2. Revisão da Literatura

“The world isn't run by weapons anymore, or energy, or money, it's run by little ones and zeroes, little bits of data. It's all just electron. […]
There's a war out there, old friend. A world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think... it's all about the information!”

– Cosmo, personagem do filme ‘Sneakers’.
(Parkes e Robinson, 1992)

2.1. Gestão da Informação

A informação representa atualmente para as organizações um recurso fundamental para o funcionamento operacional, para o desenvolvimento das suas atividades quotidianas ou ainda para garantir vantagens competitivas e facilitar a tomada de decisões estratégicas. Neste contexto, torna-se absolutamente imperativa uma correta gestão da informação. Essa gestão da informação é entendida por Wilson (1989) como sendo a gestão eficiente de todos os recursos de informação relevantes para a organização, produzidos internamente ou adquiridos externamente, recorrendo à utilização de tecnologias da informação.

No entanto, Choo (2003) faz notar que a informação se encontra, muitas vezes, fragmentada e que os detentores dessa informação não estão cientes do valor que aquela tem para a organização nem da necessidade de a partilhar e, com isso, gerar valor para a organização. Também Amaral, ao fazer uma comparação com o crescimento do interesse nas tecnologias da informação, lamentava que a Gestão da Informação "não tem beneficiado do mesmo crescendo de interesse e reconhecimento por parte da grande generalidade das organizações" (Amaral, 1994, p. 27). Davenport e Prusak (1998) sublinham que o conhecimento organizacional pertence à organização e não apenas a um grupo restrito de pessoas. Com efeito, segundo Choo (2003), a informação que é adquirida ou criada deve ser sistematicamente organizada e armazenada para facilitar a partilha e recuperação da informação.

Segundo Reis, para uma gestão da informação eficaz "[...] é necessário que se estabeleçam um conjunto de políticas coerentes que possibilitem o fornecimento de informação relevante, com qualidade suficiente, precisa, transmitida para o local certo, no tempo correto, com um custo apropriado e facilidades de acesso por parte dos utilizadores autorizados" (Reis, 1993, p. 20).

A gestão da informação é, portanto, um tema bastante complexo e que deve ter em conta as fontes de informação, internas e externas, bem como as tecnologias e processos de captura, armazenamento, distribuição, utilização, atualização e destruição dessas informações. Assim, para compreender a gestão da informação na sua plenitude torna-se necessário compreender os modelos de gestão de informação estudados por autores tão importantes, como Chun Wei Choo ou Thomas Hayes Davenport.

2.1.1. Modelo de gestão de informação de Choo

Choo (2003) propõe um modelo de gestão da informação assente em seis atividades ou processos fundamentais relacionados, que se desenrolam de forma cíclica e contínua e que devem ser convenientemente geridos:

1. *Identificação das necessidades informacionais*: as organizações procuram informações que lhes permitam resolver problemas, incertezas ou ambiguidades ou ainda melhorar comportamentos, de modo a garantir a sua sobrevivência e prosperidade, num ambiente cada vez mais hostil e incerto. As necessidades e tipologia da informação necessárias são determinadas em função da natureza dos problemas ou incertezas a resolver, tendo sempre em conta a natureza da organização, bem como a suas regras e modelo de negócio ou estilo de organização, e o contexto, como as normas profissionais vigentes ou a legislação em vigor.

   Para MacMullin e Taylor (1984) a análise das necessidades de informação não deve simplesmente determinar que informação é necessária, mas também procurar compreender o porquê da necessidade da informação, qual o problema que se pretende solucionar, que informações já são conhecidas, que informação se pretende encontrar, de que forma deve ser apresentada e de que modo irá ser usada.

   Choo (2003) enfatiza também que uma clara compreensão das verdadeiras necessidades de informação dos utilizadores está na base de um bom sistema de gestão da informação. Esta compreensão das verdadeiras necessidades de informação reveste-se de especial importância na atualidade, onde o fluxo e o ritmo de criação de informação torna imperativa a correta seleção da informação realmente útil e relevante para o utilizador.

2. *Aquisição da informação*: determinada pelas necessidades de informação, tem como objetivo satisfazê-las adequadamente. Esta poderá ser realizada internamente, recorrendo às regras e procedimentos internos, às práticas e processos correntes, regulamentação do setor e à experiência acumulada, ou a partir de fontes externas, recorrendo à consulta de bases de dados, redes de conhecimentos coletivos ou a serviços de consultoria.

   Segundo Choo (2003), a aquisição da informação deverá obedecer a um plano sistemático, alinhado com os objetivos estratégicos da organização e respeitando o princípio da variedade indispensável (Ashby, 1956), com o objetivo de garantir que aquela seja relevante, adequada, atualizada e suficiente, não pecando por excesso

nem por defeito. Davenport resume claramente este conceito ao afirmar que "A ênfase primária não está na geração e na distribuição de enormes quantidades de informação, mas no uso eficiente de uma quantia relativamente pequena" (Davenport, 2000, p. 21). Assim, a aquisição da informação representa um delicado exercício de equilíbrio entre duas necessidades opostas: se por um lado a organização requer, para o seu funcionamento, uma grande quantidade e variedade de informação, por outro é também necessário manter o volume de informação dentro do que são os limites das capacidades cognitivas humanas. Choo (2003) advoga também que as fontes de informação devem ser constantemente monitorizadas e avaliadas com o objetivo de garantir que estas satisfazem as necessidades de informação de forma relevante e contextualizada.

3. *Organização e armazenamento da informação*: com o objetivo de criar uma memória organizacional, baseada num repositório de conhecimento, a organização da informação deve assentar sobre uma estrutura que reflita os interesses e objetivos da organização e dos seus membros. A informação adquirida e produzida pela organização deverá ser sistematicamente organizada e armazenada de forma a facilitar a partilha e recuperação da informação (Choo, 2003). Assim, a organização do repositório deverá refletir as necessidades ligadas ao modelo de negócio da organização e o modo como a informação será utilizada pelos seus membros.

   Também as diversas tipologias documentais, como sejam os textos, e-mails, imagens, sons, vídeos ou outros formatos, ou ainda a necessidade de gerir diversas versões, poderão ditar diferentes estratégias de organização dos ficheiros. Uma forma de organizar os dados é através da classificação e indexação, o que permite agregar e agrupar a informação em itens facilmente representáveis de forma conveniente para os utilizadores finais. No entanto, para assegurar a correta recuperação da informação armazenada, o utilizador deve estar familiarizado com as diferentes classificações, compreender claramente o significado das diversas categorias e de que forma estas se relacionam umas com as outras (Krippendorff, 1973).

   A tecnologia atual, ao fornecer diversos métodos de estruturação e organização da informação, assume aqui um papel importante, não só como suporte para a organização e armazenamento da informação, mas também como potencial facilitador na sua recuperação, distribuição e utilização. Por último, devido à importância estratégica, patrimonial e até legal destes repositórios, deverão ser colocadas em prática rigorosa políticas de segurança, quer na vertente da gestão de

acessos e distribuição da informação, quer na vertente da contingência e reposição em caso de desastre.

Por outro lado, de forma a garantir que o volume de informação armazenada não cresce indefinidamente e se mantém apenas a informação relevante e necessária, é importante definir uma política de retenção da informação (Krippendorff, 1973). Esta política de retenção deve definir claramente que tipo de informação deve ser armazenada de forma permanente para, por exemplo, memória futura da organização; que informação deve ser mantida durante um determinado período de tempo para satisfazer, por exemplo, requisitos legais; e que informação pode ser eliminada de periódica ou sazonal.

4. *Conceção e desenvolvimento dos produtos e serviços de informação*: dado que se destinam a suprir necessidades informacionais dos diferentes utilizadores e grupos da organização, estes produtos e serviços devem ser centrados nas suas necessidades específicas, podendo, para tal, ser organizados em diferentes níveis e categorias. De acordo com Taylor (1986), cada serviço ou produto informacional deverá ser concebido de modo a acrescentar valor à informação e adaptado de acordo com o utilizador final, de modo a facilitar o processo de tomada de decisão, entender melhor uma determinada situação ou empreender ações mais efetivas. Taylor (1986) caracteriza as atividades que agregam valor à informação como sendo:
    - facilidade de utilização;
    - redução de ruídos;
    - qualidade;
    - adaptabilidade;
    - economia de tempo; e
    - economia de custos.

    Os produtos e serviços informacionais devem ser, portanto, relevantes e contribuírem para a resolução do problema, mas também ter em conta as contingências e contextos específicos que possam afetar a resolução de cada tipo de problema. Devem também garantir a qualidade da informação, melhorar a adequação e facilitar o encontro entre a informação e as necessidades dos utilizadores.

    Um sistema de informação consiste numa combinação de componentes tecnológicos, como sendo o hardware, software, redes de comunicações e dispositivos de armazenamento de dados, componentes processuais, sobe a forma de políticas, regras

e procedimentos para a aquisição, armazenamento, tratamento e distribuição da informação e o componente humano no papel de utilizador final. Nesta perspetiva, não é suficiente constituir um repositório de dados devidamente organizados e estruturados: os processos de busca de informação representam um aspeto central da interação entre o utilizador e o repositório de informação. Consequentemente, os dispositivos de recuperação de informação deverão responder de forma eficiente às solicitações do utilizador. É fundamental ter em conta a opinião e as necessidades do utilizador na conceção e desenvolvimento dos produtos e serviços de informação. O utilizador deverá também ser corretamente formado na utilização do sistema de gestão da informação (O'Brien e Marakas, 2007).

A tecnologia tem contribuído para uma maior qualidade, interatividade e flexibilidade na apresentação da informação e, ao mesmo tempo, reduzir custos e eliminar barreiras geográficas e temporais ao proporcionar uma maior rapidez na resposta às solicitações informacionais.

5. *Distribuição da informação*: Processo pelo qual a informação é distribuída pela organização, de forma a chegar ao destinatário correto, no momento e locais certos, sob a forma adequada e de acordo com as suas necessidades. Assim, um gestor de topo necessita de informação analítica, como um parecer ou uma análise de mercado, que suporte o seu processo de decisão estratégica, enquanto um operador de um equipamento poderá necessitar de informação detalhada ao nível do processo ou tarefa que executa, sob a forma de um manual de utilização ou lista de procedimentos.

   A complexidade das organizações dita a necessidade da definição de uma estratégia de distribuição da informação, de acordo com as necessidades, hábitos e preferências dos utilizadores. Esta estratégia deverá garantir que a informação chega aos utilizadores na forma correta e pelos canais apropriados, mas também que promova e incentive a pesquisa e a partilha da informação pelos próprios utilizadores, condição prévia, segundo Choo (2003), para a perceção e aprendizagem organizacional.

   Um bom sistema de distribuição da informação incentiva e facilita uma aprendizagem mais ativa na organização e aumenta as probabilidades de a informação existente ser recuperada e utilizada, o que, por sua vez, aumenta as possibilidades de aprendizagem, ao ligar informação anteriormente separada. Ainda, segundo Choo (2003), a distribuição da informação deve ser implementada de forma

adaptada aos processos de trabalho e preferências do utilizador final e focar-se no fornecimento da informação mais adequada ao desempenho das suas tarefas.

6. *Utilização da informação*: Para Choo, "O uso da informação envolve a seleção e o processamento da informação de modo a responder uma pergunta, resolver um problema, tomar uma decisão, negociar uma posição ou entender uma situação" (Choo, 2006, p. 106). O resultado do uso da informação é uma mudança no estado de conhecimento do indivíduo ou da sua capacidade de agir, um processo que ocorre de forma interativa, social e dinâmica, com vista à criação de conhecimento e à tomada de decisão. Por outro lado, o uso da informação é definido com base na experiência, vivência e educação de cada indivíduo, pelo que, ainda segundo Choo (2006), a gestão da informação deve considerar o contexto social do uso da informação, uma vez que ela ganha significado e propósito pela partilha mental e afetiva.

De acordo com o modelo de Choo (2003), a utilização da informação despoleta um comportamento adaptativo, com o qual se inicia um novo ciclo de aprendizagem, em que os resultados das ações e decisões anteriormente tomadas para atingir os objetivos retroalimentam o sistema com novas informações e conhecimentos que irão influenciar decisões futuras. Choo esquematiza o seu modelo processual de gestão da informação de acordo com a Figura 2.1, abaixo:

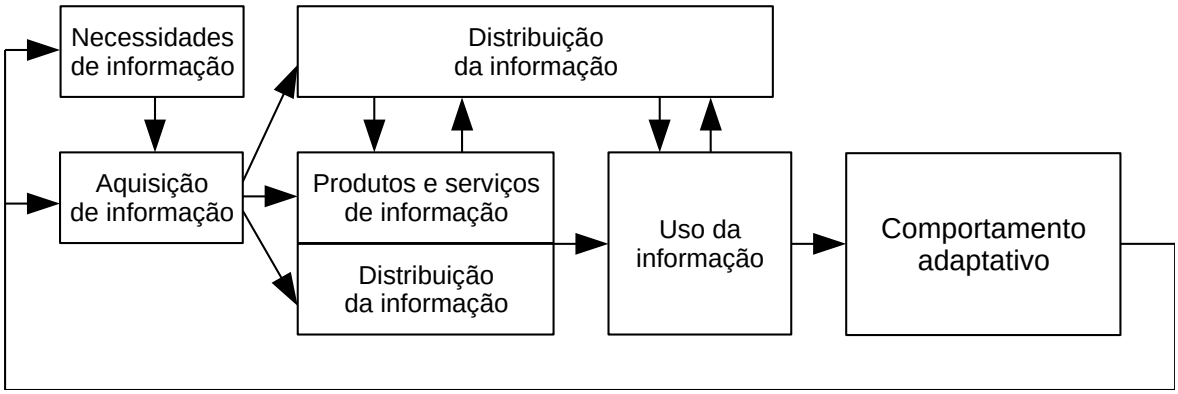


Figura 2.1: Modelo processual de gestão da informação.
Fonte: Choo (2003).

2.1.2. Modelo de gestão de informação de Davenport

Para Davenport a gestão da informação "Trata-se de um conjunto estruturado de atividades que incluem o modo como as empresas obtêm, distribuem e usam a informação e o

conhecimento" (Davenport, 2000, p. 173). O autor utiliza o termo "ecologia da informação" para ilustrar um conceito multidisciplinar de gestão da informação, centrado nas necessidades reais do utilizador, mas tendo em conta o ambiente informacional interno, o contexto e a complexa rede de relações entre as pessoas, bem como os processos e outros elementos do ambiente organizacional interno e ambiente externo de uma organização.

Continuando a sua analogia ao mundo físico, o autor destaca quatro atributos chave da ecologia da informação:

1. *A integração dos diversos tipos de informação*: como a informação estruturada e não estruturada, em suporte eletrónico ou outros, em diversos formatos, como áudio ou vídeo, é impulsionada pelas novas tecnologias e pela necessidade de melhorar o aproveitamento de formas não tradicionais de informação;
2. *O reconhecimento de mudanças evolutivas*: os sistemas de gestão da informação devem ser suficientemente flexíveis para acomodar futuras alterações ditadas pelas mudanças organizacionais;
3. *A ênfase na observação e na descrição*: dado que ninguém está totalmente familiarizado com todos os aspetos de uma organização, surge a necessidade de desenvolver mapas das informações atuais e começar a perguntar como a informação é reunida, partilhada e utilizada hoje, e o que podemos aprender com ela;
4. *A ênfase no comportamento pessoal e informacional*: um sistema de gestão de informação não deve simplesmente ser um depósito de informações, mas também facilitar o seu uso, tendo em conta as necessidade, patrões, atitudes, comportamentos e ambiente organizacionais;

Baseado nesta conceção ecológica da gestão da informação, o autor propõe um modelo processual de gestão da informação, onde importa "identificar todos os passos de um processo informacional – todas as fontes envolvidas, todas as pessoas que afetam cada passo, todos os problemas que surgem" (Davenport, 2000, p. 173). Este modelo é baseado em quatro etapas: (a) a determinação das exigências da informação; (b) a obtenção de informações; (c) a distribuição da informação; e (d) a utilização da informação.

1. *Determinação das exigências da informação*: uma das fases mais importantes do processo e onde os sistemas formais têm fracassado, dado que "para entender bem o assunto devem ser avaliadas as várias perspetivas – política, psicológica, cultural, estratégica – e as ferramentas correspondentes, como a avaliação individual e

organizacional" (Davenport, 2000, p. 176). Para um bom entendimento das necessidades de informação é importante um claro entendimento do mundo dos negócios, pelo que o autor defende a promoção de uma ampla discussão entre os fornecedores e os utilizadores da informação, mediada pelos profissionais da gestão da informação. Destaca também o papel dos analistas e a necessidade de acompanhar os gestores de forma a melhor conhecer a informação estruturada e não estruturada, a formal e informal e a computorizada e não computorizada.

2. *Obtenção de informações*: uma vez definidas as informações necessárias, inicia-se um processo contínuo, ininterrupto e nunca terminado, de obtenção de informação, através da:
    - exploração do ambiente informacional;
    - classificação da informação numa estrutura pertinente; e
    - formatação e estruturação das informações.

    O autor destaca a importância do fator humano ao afirmar que "O melhor ambiente de exploração, claro, é aquele no qual todos executam a coleta de dados e depois compartilham as informações obtidas" (Davenport, 2000, p. 184) e sustenta ainda que que as organizações obtêm as informações a partir de três fontes:

    i. *Especialistas externos*, sob a forma de publicações ou outras fontes formais;
    ii. *Fontes credíveis*, sob a forma de instituições ou indivíduos com reputação de credibilidade num determinado campo;
    iii. *Boatos internos*, onde a fonte é a própria organização.

    O autor salienta também a importância da classificação e categorização como forma de estruturar a informação e a necessidade de criar produtos e serviços de informação que apresentem as informações de forma contextualizada, num estilo e suportes adequados à classe de utilizadores a que se destina.

3. *Distribuição da informação*: diretamente ligada ao modo como a informação está formatada e armazenada, a distribuição envolve a ligação entre os gestores e os colaboradores que dela necessitam e que a usam. O autor sustenta também que a distribuição da informação é afetada por outros componentes da ecologia da informação, nomeadamente:
    - a arquitetura informacional;
    - as estruturas políticas; e

- o investimento tecnológico.

Outra decisão importante é a forma como a informação deve ser distribuída, apontando o autor duas estratégias alternativas: na primeira, a informação é divulgada aos utilizadores, que desempenham o papel de meros recetores passivos de dados, e são os gestores que decidem que informação é disponibilizada, quem a recebe, quando e em que formato. A segunda estratégia privilegia a busca da informação pelos utilizadores e considera que estes estão melhor colocados para avaliar o quê, quando e de que que forma a informação é realmente necessária e útil. Uma terceira alternativa possível, é uma forma mista das duas anteriores, em que são distribuídos ou disponibilizados mapas e guias que permitem uma melhor identificação das fontes e posterior exploração e pesquisa da informação.

4. *Utilização da informação*: uma etapa bastante pessoal, dado que a forma como o utilizador procura, absorve e usa a informação depende inteiramente dos meandros da mente humana, mas onde uma abordagem de caráter mais processual pode tornar o processo menos confuso. Esta abordagem pode ser complementada com medidas de caráter mais vinculativo, o que pode ser aperfeiçoado recorrendo a estimativas de uso da informação e ações simbólicas de promoção do uso da informação, proporcionando o contexto institucional adequado e incorporando o uso da informação nas avaliações de desempenho dos colaboradores.

O autor esquematiza as quatro etapas do processo de gestão da informação de acordo com a Figura 2.2, abaixo:

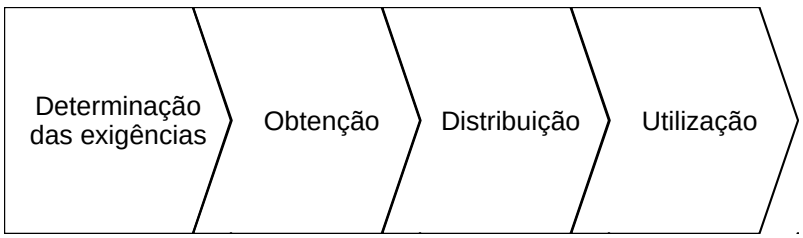


Figura 2.2: O processo de gestão da informação.
Fonte: Davenport (2000, p. 175)

2.1.3. Classificação da informação

Sabine Mas (2007) salienta a importância da aplicação dos princípios teóricos da classificação documental como base para a conceção de um sistema eficaz de classificação

da informação. Uma das principais funções da classificação da informação é a de permitir agrupar informação relativa a um determinado assunto e facilitar assim o seu armazenamento físico ou eletrónico. Não menos importante é o papel que a classificação desempenha na busca de informação, ao fornecer ao utilizador uma contextualização do assunto da pesquisa. Deste modo, o utilizador pode iniciar a pesquisa de informação a partir de uma classificação mais ampla e, progressivamente, ir afinando a sua pesquisa, balizando-a dentro de classes cada vez mais específicas, o que permite encontrar respostas cada vez mais pertinentes para sua questão inicial. A classificação tem, portanto, um duplo papel, sendo essencial quer para a organização da informação, quer para a sua busca e utilização. No entanto, a classificação é também um importante auxiliar nas restantes etapas do ciclo da gestão da informação, ao facilitar as atividades de criação, organização, armazenamento, recuperação, utilização, retenção e destruição da informação.

Segundo Mas (2007), a classificação, definida em termos gerais, consiste em agrupar determinados elementos em classes, com base nas suas qualidades, atributos ou caraterísticas comuns, de tal forma que entidades semelhantes se encontrem agrupadas e, por consequência, separadas de entidades que não apresentem as mesmas semelhanças. Couture (1999) descreve a classificação como sendo um processo intelectual de identificação e agrupamento sistemático de elementos semelhantes a partir das suas caraterísticas comuns.

A definição adotada pelo International Records Management Trust[1] (IRMT) refere a classificação como uma ferramenta hierárquica que visa facilitar a captura, titulação, recuperação, bem como as regras de retenção e destruição da informação e que, quando usada em ambiente eletrónico, deve também permitir a busca e recuperação dos registos e metadados associados. (Keakopa et al., 2009).

Couture (1999) faz depender também a classificação do número de elementos, salientando que, nos casos em que a quantidade assim o exija, os elementos de uma classe poderão ser recursivamente reagrupados em subclasses cada vez mais específicas.

Um princípio que é transversal a diversos autores (Couture, 1999; Charbonneau e Robert, 2001; Mas, 2007; Collet, 2012) é a importância de, na conceção de um esquema de classificação da informação, partir do geral para o particular. Por consequência, a estrutura de um esquema de classificação pode variar em função das necessidades da organização e

1 http://www.irmt.org

da aplicação da informação. Assim, uma classificação pode ser concebida numa perspetiva mais filosófica, em função dos domínios do conhecimento (como as artes ou as ciências) ou numa vertente mais profissional, em função das áreas de atuação ou subdivisões funcionais de uma organização (como a contabilidade ou os recursos humanos).

Mas (2007) defende que o processo de elaboração de uma classificação deve passar por duas etapas principais: a identificação e ordenação das classes e a escolha da notação a utilizar. Especial cuidado deve ser colocado na definição das características que determinam o primeiro nível de classificação (macroestrutura). Dado que uma determinada informação pode ser enquadrada em diversas classes, em função, por exemplo do tema tratado, do tipo de documento ou da atividade a que se refere, é importante que a classificação seja efetuada à luz de um único critério e uma única caraterística da informação, de forma a garantir o princípio da exclusividade das classes e evitar que um determinado objeto possa ser catalogado sob duas ou mais classes. Por outro lado, é essencial que a classificação seja exaustiva, de forma a contemplar todas as possibilidades e garantir que todos os objetos possam ser enquadrados numa classe. A propósito desta necessidade, Davenport utiliza a expressão "MECE: mutuamente exclusivas, coletivamente exaustivas" (Davenport, 2000, p. 185). O mesmo cuidado e critérios deverão ser aplicados na definição das sub-classes (microestrutura), de forma a assegurar a homogeneidade e previsibilidade da classificação.

A norma ISO 15489 (2016) recomenda que as classes descrevam as funções e atividades da organização, refletindo os seus processos de negócios. Segundo esta norma, o nível superior da classificação deve descrever as principais funções da organização, enquanto o segundo nível pode descrever subfunções e, num terceiro nível, são descritos os processos, ou seja, as atividades que são constantemente repetidas.

Também para Collet (2012) a definição de classificação está intimamente ligada à estrutura funcional das organizações, ao defender que o plano de classificação é constituído por classes, organizadas hierarquicamente, de forma a representar as atividades da organização. Como este tipo de classificação reflete as atividades desenvolvidas pela organização, que são relativamente estáveis ao longo do tempo, a pesquisa e recuperação da informação é facilitada, dado o conhecimento que os utilizadores possuem sobre a instituição. Paralelamente, um esquema de classificação em função das atividades da organização facilita a compreensão do contexto de criação e utilização da informação no seio da organização, acrescentando-lhe valor.

O próprio valor da informação para a organização pode ser refletido no esquema de classificação. Amaral (1994) propõe uma classificação que permite separar a informação relevante e valiosa da informação sem qualquer valor para a organização. Assim, o autor categoriza a informação em quatro níveis:

1. *lixo*, como sendo a informação sem qualquer valor para a organização;
2. *potencial*, quando o uso a informação permite obter vantagens competitivas;
3. *mínima*, quando é essencial para uma boa gestão da organização; e
4. *crítica*, para toda a informação que é essencial para a sobrevivência da organização.

Esta classificação é representada pela Figura 2.3, abaixo.

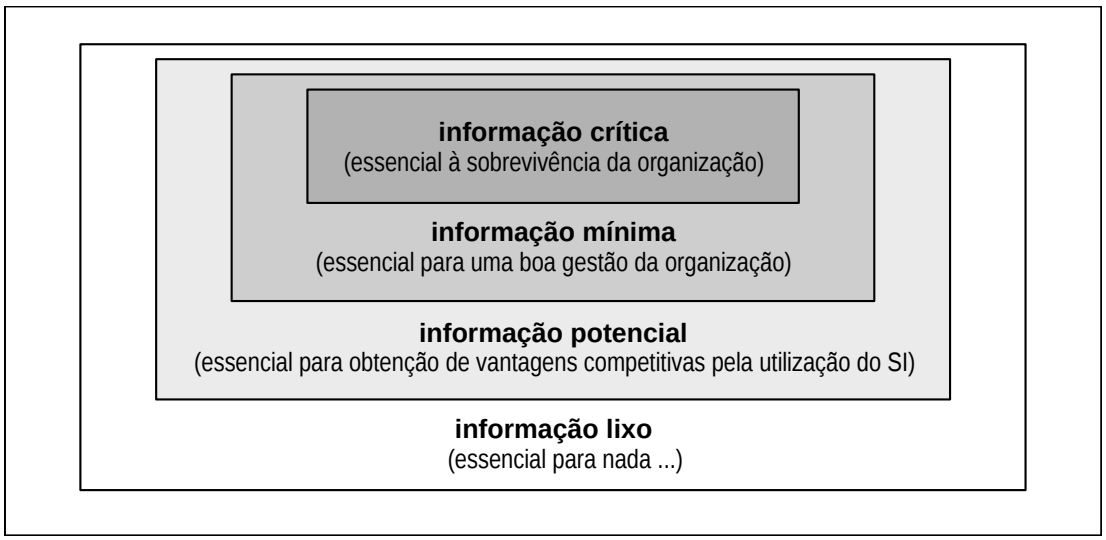


Figura 2.3: Classes da Informação.
Fonte: Amaral (1994, p. 29)

Relativamente à notação, Mas (2007) define-a como sendo um conjunto de símbolos, compostos por letras, números ou outros símbolos tipográficos, que permitem uma representação sintética e abstrata dos assuntos representados no esquema de classificação. Para a autora, a notação tem um papel essencial na organização da informação, ao facilitar o seu armazenamento e recuperação, e deve possuir as seguintes qualidades:

- *Familiar*: a notação deve utilizar símbolos familiares, de fácil leitura, pronúncia, compreensão e memorização por parte do utilizador;
- *Lógica*: a notação deve refletir a ordem da classificação e expressar os níveis de especificidade de cada classe;
- *Flexível*: a notação dever ser suficientemente flexível de forma a permitir a expansão de esquema e a integração de novos conceitos;

A autora compila também, a partir da literatura existente, um conjunto de propriedades que um plano de classificação deve contemplar:

- *Simplicidade*: o esquema de classificação deve ser rapidamente compreendido e assimilado pelos utilizadores. A sua estrutura deve ser composta por três a quatro níveis e os termos utilizados para designar as classes devem ser concisos e coerentes, de forma a evitar ambiguidades;
- *Lógica*: o esquema de classificação deve cobrir todos os assuntos ou áreas de atividade de forma exaustiva, exclusiva e coerente, utilizando apenas uma caraterística para a classificação em cada nível hierárquico e possibilitar uma pesquisa de forma lógica e metódica, partindo do geral para o particular;
- *Hospitalidade*: o esquema de classificação deve refletir a evolução das atividades da organização e permitir a incorporação de novas subclasses, mantendo, ao mesmo tempo, a sua estabilidade e estrutura lógica;
- *Autoridade*: o esquema de classificação deve ser edificado sobre uma base consensual, de forma a garantir a acessibilidade, aceitação e adoção por parte dos utilizadores;
- *Universalidade*: o esquema de classificação deve ser passível de utilização em qualquer aplicação ou contexto e de forma transversal, de modo a garantir a uniformização da classificação da informação na organização, independentemente do seu suporte.

Com o passar do tempo, o número de arquivos aumentará gradualmente. Também naturalmente, com o decorrer do tempo, algumas das informações mais antigas perderão o seu valor e a sua relevância. Em contrapartida, informações haverá que, por razões legais, históricas ou outras, deverão ser preservadas por períodos mais longos ou mesmo indefinidamente. Assim, haverá material que deve ser preservado por mais tempo, e também haverá material que pode ser eliminado após um curto período de tempo. Em muitos casos, o tempo de conservação será estabelecido pelas leis e regulamentos vigentes.

Entender quais as informações a manter e quais as informações que já não são necessárias e poderão ser descartadas é uma parte importante da gestão eficaz da informação. No entanto, a eliminação deve ser feita de forma responsável através de uma compreensão clara das funções e objetivos de uma organização, do valor das informações para o negócio e dos requisitos de retenção da informação imposto pela legislação. Também a destruição

da informação sensível para a organização, como a classificada como *confidencial* ou *reservada*, deve ser levada a cabo com especial cuidado, de forma a garantir que o método de destruição não deixe margem para uma eventual recuperação da informação por pessoas não autorizadas.

2.2. Dados, informação e conhecimento

Davenport (2000), bem como Stair e Reynolds (2012), sublinham a distinção entre dados, informação e conhecimento. Assim,

- *Dados*: consistem, simplesmente, em factos crus. Os dados são facilmente estruturados, gerados, capturados e armazenados por máquinas, no seu estado bruto, sem qualquer tratamento e ou significado.
- *Informação*: consiste numa coleção de factos organizados de tal forma que atribui relevância e acrescenta valor aos factos individuais. Peter Drucker (1998) define informação como sendo dados dotados de uma relevância e um propósito. A criação de informação a partir de dados requer análise, consenso quanto ao significado atribuído e intervenção humana para o seu processamento, sob forma da aplicação de conhecimentos. Para Stair e Reynolds (2012) o valor da informação está ligado à forma como auxilia os tomadores de decisões a atingir os objetivos da organização. Por seu lado, Davenport (2000) adverte que, ao contrário dos dados, a informação é de muito mais difícil transmissão com absoluta fidelidade.
- *Conhecimento*: é, para Stair e Reynolds (2012), a consciência e compreensão de um conjunto de informações e as formas como essa informação pode ser utilizada para apoiar uma tarefa específica ou tomar uma decisão. Davenport e Prusak (1998) definem o conhecimento como sendo uma síntese de múltiplas fontes de informação. O conhecimento é dificilmente estruturado, gerado ou capturado por máquinas. Sendo uma construção da mente humana, o conhecimento inclui análise, síntese, reflexão e juízo crítico, revestindo-se frequentemente de um caráter tácito e contextual que dificulta a sua transferência. O conhecimento é valioso porque "alguém deu à informação um contexto, um significado, uma interpretação; alguém refletiu sobre o conhecimento, acrescentou a ele sua própria sabedoria, considerou suas implicações mais amplas." (Davenport, 2000, p. 19)

A Tabela 2.1, abaixo, sintetiza as principais diferenças, na perspetiva de Davenport, entre dados, informação e conhecimento.

Tabela 2.1: Dados, informação e conhecimento.
Fonte: Davenport (2000, p. 18).

Dados	**Informação**	**Conhecimento**
Simples observações sobre o estado do mundo. • Facilmente estruturados • Facilmente obtidos por máquinas • Frequentemente quantificados • Facilmente transferíveis	Dados dotados de relevância e propósito. • Requer unidade e análise • Exige consenso em relação ao significado • Exige necessariamente a mediação humana	Informação valiosa da mente humana. • Inclui reflexão, síntese e contextos • De difícil estruturação • De difícil captura por máquinas • Frequentemente tácito • De difícil transferência

Convém salientar que apenas a informação e o conhecimento, e não os dados simples, poderão catalisar evoluções no conhecimento e modificações de comportamentos nas organizações.

Os autores, enumeram ainda diferentes tipos de dados, como sendo:

- *Alfanuméricos*, representados por números, textos ou outros carateres.
- *Imagens*, compostos por gráficos ou fotografias.
- *Áudio*, na forma de sons, ruídos ou registos sonoros.
- *Vídeo*, representados por imagens em movimento.

Para Stair e Reynolds (2012), os dados representam, por si só, o mundo real e apenas adquirem significado após passarem por um processo de transformação. Assim, os dados são transformados em informação útil ao serem selecionados, manipulados e organizados de forma a acrescentar valor ao conjunto. Esse pode ser um processo mental ou manual ou, ainda, recorrendo a ferramentas informáticas. Durante o processo de transformação, os dados são selecionados ou rejeitados de acordo com a sua importância e relevância, através da aplicação do conhecimento adquirido anteriormente. Deste modo, os autores demonstram que o processo de transformação consiste na aplicação de conhecimento aos dados como forma de os transformar em informação útil.

Ainda relativamente à qualidade e utilidade da informação, Stair e Reynolds (2012) enumeram um conjunto de características que tornam a informação valiosa:

- *Acessíveis*, de fácil acesso aos utilizadores autorizados, no formato correto e no momento exato em que delas necessitam.

- *Precisas*, na medida em que não contem erros ou lixo que deve ser filtrado no processo de transformação.
- *Completas*, contendo todos os factos importantes.
- *Económicas*, na medida em que o custo de produção deve ser relativamente económico, não se sobrepondo ao valor da própria informação.
- *Flexíveis*, na medida em que podem ser utilizadas para diversos propósitos.
- *Relevantes*, demonstrando a sua importância no contexto da tomada de decisão.
- *Confiáveis*, na medida em que devem ser verdadeiras e de confiança.
- *Seguras*, de modo a estarem resguardadas de acessos não autorizados.
- *Simples*, de modo a evitar excesso de informação que dificulte a tarefa ao tomador de decisão.
- *Atempadas*, estando disponíveis no momento exato em que são necessárias.
- *Verificáveis*, possibilitando uma comprovação da sua veracidade.

No entanto, Stair e Reynolds (2012), sublinham também que a utilidade da informação pode variar largamente em função da proporção de cada um desses atributos ou em função da valorização que a organização ou o utilizador atribui a cada um. Assim, para um gestor, pode ser essencial dispor de projeções de mercado atempadas, ainda que com alguma margem de erro. O valor da informação está diretamente ligado ao modo como esta contribui, no processo de tomada de decisão, para que a organização atinja os seus objetivos.

2.3. Trabalho colaborativo

Nos últimos anos, tem-se vindo a assistir a uma crescente valorização da cultura da colaboração, do trabalho em equipa e das comunidades profissionais de prática nas organizações, o que coloca em evidência a emergência da colaboração como um fenómeno contemporâneo (Tractenberg & Struchiner, 2010). De facto, ainda segundo os mesmos autores, nas últimas duas décadas, o “saber trabalhar em equipa” ou a “capacidade de trabalhar em grupo” representam os atributos mais importantes de quem quer ingressar ou manter-se no mercado de trabalho e dos requisitos de topo para a contratação de colaboradores pelas empresas, o que é corroborado por Isabel Alarcão quando defende que “a rápida evolução dos conhecimentos, conjugada com a igualmente rápida evolução das

necessidades da sociedade, exigem de todos uma permanente aprendizagem individual e colaborativa" (Alarcão, 2003, p. 16).

O trabalho colaborativo consiste, na perspetiva de Stewart, "num processo que envolve pessoas de diferentes contextos, com diferentes vivências e experiências profissionais, trabalhando conjuntamente, como iguais, tendo em vista benefícios mútuos" (Stewart, 1997, p. 31). Boavida e Ponte (2002) sublinham que só se pode falar em colaboração quando os intervenientes trabalham em conjunto, sem hierarquias e numa base de igualdade, de modo a haver ajuda mútua na persecução de objetivos em que todos beneficiem.

A importância dos benefícios mútuos como resultado da colaboração é fundamental para Lima, que os distingue dos resultados da cooperação quando afirma que "na cooperação, as acções de cada indivíduo podem ser agradáveis para o outro mas não resultam necessariamente em benefícios mútuos" (Lima, 2002, p46), enquanto "na colaboração, cada indivíduo participa com a sua parte num empreendimento comum cujo resultado beneficia todas as pessoas envolvidas" (Lima, 2002, p46). Também Boavida e Ponte defendem que "subjacente à ideia de colaboração está, também, uma certa mutualidade na relação: todos têm algo a dar e algo a receber do trabalho conjunto" (Boavida e Ponte, 2002, p. 6), sublinhando assim a importância do equilíbrio da relação.

Num ambiente colaborativo, onde a chave é a interação entre os participantes, as questões de inter-relacionamento pessoal assumem uma importância acrescida. Boavida e Ponte (2002) sublinham três aspetos fundamentais para o sucesso de um projeto colaborativo: a confiança, o diálogo e a negociação.

- *Confiança*, assente num clima de respeito e cuidado, quer a nível pessoal, quer a nível profissional, é uma condição fundamental para que os participantes possam questionar e discutir abertamente ideias, valores e ações uns dos outros, com a confiança que o seu trabalho será igualmente escrutinado, mas também respeitado. A confiança está associada à capacidade de saber ouvir os outros e valorizar as suas contribuições e a um forte sentimento de pertença ao grupo.
- *Diálogo*, baseado na premissa que cada voz pode e deve ser ouvida, mas também que nenhuma ideia é absoluta e definitiva. Através do diálogo, a compreensão torna-se mais rica e mais informada, propiciando o estabelecimento de consensos e visões comuns. Os autores sublinham também a importância do diálogo como instrumento

para anular contradições, permitir o confronto de ideias e fomentar construções de novas compreensões.

- *Negociação*, omnipresente no projeto de colaboração e apontada como a chave para uma colaboração bem-sucedida, é fundamental para a resolução de momentos de impasse ou de crise. Num projeto colaborativo, "é preciso ser capaz de negociar objectivos, modos de trabalho, modos de relacionamento, prioridades e até significados de conceitos fundamentais." (Boavida e Ponte, 2002, p. 7)

Gray (1989) define duas vias para a colaboração: uma, com interesse em resolver ou negociar conflitos e outra com o intuito de realizar ou atingir uma visão ou objetivos comuns. A autora identifica, também, dois tipos de resultados da colaboração: troca de informação e acordos comuns. A mesma autora enumera ainda cinco caraterísticas que considera críticas para a colaboração:

1. os intervenientes são interdependentes;
2. as soluções emergem ao lidarem de forma construtiva com as suas diferenças;
3. a propriedade conjunta das soluções;
4. os intervenientes assumem responsabilidade coletiva pelo rumo das suas decisões;
5. a colaboração é um processo emergente.

A autora sublinha a capacidade de os intervenientes lidarem com as suas diferenças, de forma construtiva, como o requisito fulcral para o sucesso da colaboração. De facto, também Tractenberg e Struchiner (2010) defendem que o estabelecimento de uma verdadeira cultura de colaboração implica não só o desenvolvimento de habilidades interpessoais, mas também a mudança de crenças sobre o trabalho em conjunto e a criação de laços afetivos e de confiança entre os diversos atores. Lima (2002) nota que ainda que cada indivíduo participe com o seu contributo individual para um objetivo comum, que beneficia todos os envolvidos, a responsabilidade pelo processo é partilhada, dado que as decisões criticas são tomadas em conjunto.

Convém sublinhar, porém, que a existência de uma cultura colaborativa pode não conduzir, por si só, a uma evolução qualitativa da aprendizagem e das práticas da organização. Se a comunidade colaborativa for composta por um número reduzido de membros e não facilitar ou promover a inclusão de novos participantes, poderá simplesmente perder o seu caráter inovador e estagnar num circulo sem evolução, reduzindo, à partida, possibilidades de aprendizagem e adaptação a novas situações.

Os fenómenos e práticas colaborativas atuais estão intimamente relacionadas com as novas Tecnologias da Informação e Comunicação (TIC), nomeadamente, a internet, onde estão disponíveis diversas ferramentas de publicação colaborativa, de fácil acesso e utilização. O'Reilly (2005) apadrinha o termo "web 2.0" para definir a mudança de paradigma em que o utilizador da internet deixa de ter uma posição passiva de consumidor de conteúdos e passa, ele próprio, a participar ativamente na produção e partilha de novos conteúdos, de forma colaborativa. A web 2.0 permite a comunicação bidirecional entre o site e os utilizadores e refere-se a um conceito que permite que os indivíduos colaborem uns com os outros e contribuam para a autoria de conteúdo, personalizar sites para seu uso e publicar instantaneamente os seus conteúdos (Frunzeanu, 2015). Esta facilidade de colaboração online e partilha entre utilizadores, facilitadas por interfaces convenientes, agradáveis, intuitivas e convivais, tiveram traduziu-se a imensa popularidade dos sites de partilha e redes sociais que atualmente se pode verificar.

Com desenvolvimento da web 2.0 e numa época em que a internet se vai tornando virtualmente omnipresente e instantaneamente disponível, esta tende a ser vista, cada vez mais, como um meio privilegiado para a partilha de informação e a colaboração. Como consequência, as organizações aproveitam cada vez mais a internet para criar uma cadeia de valor virtual onde indivíduos e parceiros de negócios podem comunicar e colaborar entre si. Para além disso, a tecnologia Web Services, que possibilita a interoperabilidade entre aplicações através da rede e usando protocolos abertos, emergiu como uma ferramenta promissora para integrar fontes de informação distribuídas e funcionalidades de software de uma forma flexível, escalável, reutilizável e económica. Esta tecnologia permite uma abordagem orientada a serviços para a integração de informações e aplicações distribuídas numa rede à qual os utilizadores se podem ligar (Su e Chiang, 2012).

2.4. Segurança da Informação

Sendo um dos ativos mais importantes de qualquer organização, a informação deve ser adequadamente preservada e protegida. Por outro lado, a grande conetividade e mobilidade proporcionadas pelas novas tecnologias e equipamentos, apesar das inegáveis vantagens que oferecem, fazem com que a informação esteja, agora mais do que nunca, exposta a uma quantidade e diversidade crescentes de ameaças e vulnerabilidades. Deste modo, a segurança torna-se um fator crítico na gestão da informação.

Peixoto defende que “o termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo a sua não disponibilidade” (Peixoto, 2006, p. 37). Beal define a segurança da informação como sendo “o processo de proteger a informação das ameaças para garantir a sua integridade, disponibilidade e confidencialidade” (Beal, 2005, p. 71).

2.4.1. Pilares da segurança da informação

Assim, e de acordo com os diversos autores citados, podemos considerar as pedras basilares da segurança da informação como sendo:

- *Confidencialidade*: a garantia que o acesso à informação está limitado aos utilizadores, entidades ou sistemas devidamente autorizados e protegida contra acessos indevidos. A confidencialidade é uma condição necessária para a proteção da privacidade dos utilizadores e da organização.
- *Integridade*: a informação é exata, mantém todas as suas caraterísticas originais e não foi alterada, de forma indevida, no percurso entre o emissor e o recetor. A integridade garante que a informação não foi alterada sem a devida autorização.
- *Disponibilidade*: a garantia que a informação está disponível, para as entidades autorizadas e para uso legítimo, no momento em que for necessária. Sistemas de alta disponibilidade garantem um elevado grau de disponibilidade da informação recorrendo, por exemplo, à redundância dos elementos críticos do sistema.

Camp (2001) e Adachi (2004) referem a preservação da integridade, confidencialidade, disponibilidade e acrescentam ainda a autenticidade, o não repúdio e a privacidade como sendo características fundamentais da segurança da informação.

- *Autenticidade*: a garantia que a informação é autentica, com origem na fonte que declara ser e que não foi alterada após o envio ou receção. O conceito abrange também a garantia da identidade do emissor e do recetor. Esta garantia pode requerer a utilização de certificados ou assinaturas digitais.
- *Não repúdio*: a garantia que um sistema ou utilizador efetuou uma operação, não suscitando dúvidas quanto à sua autoria ou realização, nem podendo o emissor nem o recetor negar tal facto. Esta é uma condição necessária para a validação jurídica da informação e das transações digitais.

- *Privacidade*: a garantia de proteção e não divulgação de informação pessoal ou da esfera privada do indivíduo.

Sêmola (2003) acrescenta também a legalidade da informação:

- *Legalidade*: a garantia que toda a informação foi produzida ou adquirida em conformidade com a legislação em vigor.

A segurança da informação compreende, portanto, todos os mecanismos e medidas colocadas em prática com objetivo de garantir e assegurar a confidencialidade, integridade, disponibilidade, autenticidade e não repúdio da informação e dos sistemas de informação, e que visam evitar ameaças como a revelação de informações de modo não autorizado, a ocorrência de fraudes, a interrupção dos serviços ou a usurpação da informação.

A segurança da informação é também um processo dinâmico, que deve ser continuamente monitorizado e melhorado. A norma ISO/IEC 27001 (2013) especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação dentro do contexto da organização. Também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação à medida das necessidades da organização. Os requisitos inscritos na norma são intencionalmente genéricos e destinam-se a ser aplicáveis a todas as organizações, independentemente do seu tipo, tamanho ou natureza.

A norma ISO/IEC 27001 (2013) determina que a organização deve estabelecer, implementar, manter e melhorar continuamente a segurança dos seus sistemas de informação. A norma estabelece que a proteção da informação deve também contemplar duas vertentes indissociáveis: a vertente da preservação da confidencialidade, integridade e disponibilidade da informação e a vertente da garantia da continuidade do negócio. Para tal, a norma determina que a conceção e planeamento de um sistema de segurança de informação deva ter em conta:

- O *entendimento da organização e do seu contexto*: A organização deve determinar as questões externas e internas que são relevantes para os seus objetivos e que afetam a sua capacidade de alcançar os resultados pretendidos pelo seu sistema de gestão da segurança da informação.
- As *necessidades e expetativas de todas as partes interessadas*: A organização deve determinar: (a) as partes interessadas relevantes para o sistema de gestão da

segurança da informação e (b) os requisitos destas partes interessadas relevantes para a segurança da informação.

Ainda a mesma norma refere que o planeamento de um sistema de segurança da informação deve determinar os riscos e oportunidades que devem ser abordados para:

- Garantir que o sistema de gestão da segurança da informação possa atingir os resultados pretendidos,
- Prevenir ou reduzir os efeitos indesejáveis e
- Garantir uma melhoria contínua.

2.4.2. Camadas da segurança da informação

Sêmola (2003) e também Araújo (2005) referem que a segurança da informação deve ser gerida nas perspetivas física, tecnológica e humana. Assim, as diferentes ameaças podem ser classificadas em três grandes categorias:

- *Físicas*: sejam resultantes de fenómenos ou catástrofes naturais, como tempestades, incêndios, inundações, terramotos, descargas elétricas ou cortes de energia ou ainda resultantes de atos deliberados e ações criminosas, como vandalismo, incêndios criminosos ou outros tipos de ataques às instalações físicas.
- *Tecnológicas*: resultantes de ataques deliberados causados por agentes humanos, como hackers ou vírus, mas também com origem em falhas técnicas ou defeitos de hardware ou software, como o desgaste do hardware ou dos suportes digitais ou a obsolescência do software;
- *Humanas*: decorrentes de atos intencionais, com o objetivo de causar perdas ou danos, como roubos, fraudes, espionagem industrial ou sabotagem ou ainda de atos não intencionais ou involuntários, como a deficiente utilização do sistema ou das medidas de segurança.

O perímetro de atuação da segurança da informação é, assim, bastante vasto e multidisciplinar, abrangendo áreas que vão desde a infraestrutura física e tecnológica até ao fator humano. Por este motivo, Adachi (2004), preconiza que a gestão da segurança da informação é classificada em três camadas: física, lógica e humana.

- *Camada física*: o ambiente onde o hardware está fisicamente localizado. Refere-se não apenas aos equipamentos, como os servidores, aos componentes, como os discos e circuitos, aos periféricos, como as impressoras, mas também a toda a infraestrutura

de rede, telecomunicações e de transmissão de dados. Para mitigar os riscos da camada física recorre-se a várias medidas, como o controlo de acessos, senhas de acesso, cartões ou biometria; escolha criteriosa da localização, com vista a minimizar riscos de catástrofes naturais, como sismos e inundações; sistemas de deteção e proteção de acidentes, como a deteção e extinção de incêndios; sistemas de videovigilância e deteção de intrusões; equipas de assistência e manutenção permanentes; monitorização dos parâmetros críticos como a temperatura, humidade ou o nível de ruído; redundância de equipamentos, componentes e periféricos.

- *Camada lógica*: constituída pelo software utilizado para gerir, manter e aceder ao sistema de informação. Deve ser entendida como sendo o software de base ou sistema operativo, as aplicações diretamente responsáveis pela gestão, funcionamento e acesso ao sistema de informações, mas também todo o software utilizado para garantir a segurança do sistema, como as aplicações de encriptação e decriptação de dados, os sistemas de gestão e controlo de assinaturas e certificados digitais, de credenciais e controlo de acessos, as aplicações de deteção de intrusão, antivírus, *firewalls*, bem como as aplicações que monitorizam o bom funcionamento do sistema, facilitando a deteção e prevenção de falhas físicas ou lógicas.
- *Camada humana*: constituída pelos recursos humanos envolvidos na execução, manutenção e utilização do sistema de informação. Nesta camada, estão englobados os recursos humanos da empresa e o utilizador final bem como os processos operacionais, as políticas de segurança adotadas e o nível de formação e consciencialização desses recursos humanos. Araújo (2005, p. 5) salienta que “o factor humano é o principal desafio para se ter uma boa e segura conduta de Segurança da Informação”. Nesta área, é importante a definição clara e observação das regras e padrões de segurança, a gestão, formação e sensibilização dos recursos humanos, auditoria dos registos de eventos, monitorização das mudanças e ocorrência de problemas, agir de forma ética e responsável, compreender, cumprir e fazer cumprir a legislação aplicada, ser capaz de detetar a ocorrência de irregularidades, preservar elementos probatórios e colaborar com a autoridade, analisar o impacto para a organização e para o negócio, da ocorrência de desastre natural ou falha humana e determinar, desenvolver e implementar planos de mitigação, de contingência, de continuidade e de recuperação.

Netto e Silveira (2007) agrupam as secções da norma ISO/IEC 27002 (2005) nas mesmas três camadas física, lógica e humana, na forma esquematizada na Tabela 2.2, abaixo.

Tabela 2.2: Secções da norma ISO IEC 27002 por camadas.
Fonte: Netto e Silveira (2007).

Camada	Secção	Objetivos
Física	Gestão das operações e comunicações	• Garantir a operação segura e correta dos recursos de processamento da informação.
	Segurança física e do ambiente	• Prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização; impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.
	Controle de acesso	• Controlar o acesso à informação; assegurar acesso de utilizadores autorizados e prevenir acesso não autorizado a sistemas de informação; prevenir o acesso não autorizado dos utilizadores e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação; prevenir acesso não autorizado aos serviços da rede.
	Gestão de incidentes de segurança da informação	• Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes da segurança da informação.
Lógica	Aquisição, desenvolvimento e manutenção de sistemas de informação	• Garantir que segurança é parte integrante de sistemas de informação; prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações; proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos; • Garantir a segurança de arquivos de sistema; manter a segurança de sistemas aplicativos e da informação. • Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
Humana	Organizando a segurança da informação	• Gerir a segurança de informação dentro da organização; manter a segurança dos recursos de processamento da informação e da informação da organização, que são acedidos, processados, comunicados ou geridos por partes externas.
	Gestão de Ativos	• Alcançar e manter a proteção adequada dos ativos da organização; assegurar que a informação receba um nível adequado de proteção.
	Segurança em recursos humanos	• Assegurar que os funcionários, fornecedores e terceiros entendam as suas responsabilidades e estejam de acordo com os seus papeis e reduzir o risco de roubos, fraudes ou mau uso de recursos.
	Gestão da continuidade do negócio	• Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso.
	Conformidade	• Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
	Política de segurança da informação	• Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes

As ameaças podem ser de natureza diversa, podendo também ser classificadas como passivas, ativas, maliciosas e não maliciosas. De modo a lidar de forma eficaz com estas ameaças, torna-se necessário a definição e implementação de políticas e mecanismos de segurança que visem garantir a:

- *Prevenção*, evitando a violação das medidas e mecanismos de segurança;
- *Deteção* de violações dos mecanismos de segurança;
- *Recuperação*, de modo a interromper e conter a ameaça, avaliar e reparar eventuais danos e garantir a operacionalidade do sistema e a continuidade do negócio em caso de violação das medidas de segurança.

2.4.3. Criticidade da informação

A gestão da segurança da informação deve contribuir ativamente para a manutenção das principais características da informação, como a confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio. Desta forma, a informação pode também ser classificada de acordo com o seu valor, os seus requisitos legais ou a sua sensibilidade e criticidade para a organização.

Uma política de classificação da informação fornece uma forma de garantir que as informações confidenciais sejam tratadas de acordo com o risco que ela representa para a organização. Dentro dos requisitos de confidencialidade, Beal (2005) postula a classificação da informação em três níveis: *confidencial*, *reservada* ou *interna* e *pública*.

- *Confidencial*: toda a informação cuja divulgação ou acesso não autorizado possa causar danos graves à organização. Esta classificação aplica-se a toda a informação utilizada em processos sensíveis, cuja divulgação, modificação ou destruição não autorizada afete negativamente a organização, os seus clientes, fornecedores, funcionários ou parceiros de negócio. Informações sobre a propriedade intelectual, negociações de contratos, a maioria das questões relacionadas com recursos humanos, informações de identificação dos colaboradores, dados de saúde protegidos, números de contas bancárias e informações de cartão de pagamento de clientes e funcionários são exemplos de informações confidenciais.
- *Reservada* ou *interna*: englobando toda a informação utilizada nos processos de negócio, que deve ser apenas do conhecimento de um grupo restrito de pessoas internas à organização e cuja divulgação, modificação, destruição ou acesso não

autorizado possa, de alguma forma, comprometer o alcance de objetivos ou metas da organização ou possa ainda afetar, de alguma forma, os seus clientes, fornecedores, colaboradores ou parceiros de negócio. Enquadram-se nesta categoria, a título de exemplo, os manuais de procedimentos e políticas internas ou as listas de contactos da organização.

- *Pública*: informação de livre acesso e de divulgação pública. Esta classificação aplica-se a informações produzidas ou adquiridas com o objetivo de serem disponibilizadas ao público em geral e destinadas a serem distribuídas fora de uma organização. Esta informação pode ser livremente distribuída sem risco de danos. Engloba qualquer informação que é produzida para consumo público, como comunicados de imprensa, anúncios de emprego e folhetos de vendas e todo o material de marketing e publicidade.

No que diz respeito aos requisitos de disponibilidade, Beal (2005) sugere uma classificação de acordo com o impacto que a sua falta possa ter para a organização e categorizando-a de acordo com o tempo necessário para a sua recuperação. Quanto aos requisitos de autenticidade, a mesma autora propõe uma classificação em função da exigência de verificação da autenticidade e procedência da informação antes do seu uso.

Araújo (2005) sublinha que esta classificação não é estática e pode evoluir ao longo do tempo ou de acordo com alguma política predeterminada. Assim, uma informação que, numa determinada data, foi classificada como confidencial, pode evoluir para interna ou para pública. Do mesmo modo, a informação pode perder ou adquirir valor ao longo do tempo. Consequentemente, a norma ISO/IEC 27002 (2013) define que a classificação da informação deve ser revista e avaliada periodicamente, considerando os seus requisitos de confidencialidade, integridade e disponibilidade, e atualizada de acordo com as necessidades, circunstâncias ou política previamente estabelecida. A norma postula também que o esquema de classificação da informação deve ser consistente e uniformizado em toda a organização e integrado nos seus métodos e processos, de forma a refletir o valor que a informação representa para a organização e estar alinhado de acordo com a política de controlo de acessos.

2.4.4. Política de segurança da informação

De forma a garantir a segurança da informação, as organizações devem definir e colocar em prática uma política de segurança da informação que forneça, de forma clara,

estruturada e inequívoca, orientações e regras necessárias para a proteção eficaz de todos os ativos de informação da organização. Para Araújo (2005), a Política de Segurança da Informação (PSI) “deve incluir regras detalhadas, definindo como as informações e os recursos da organização devem ser manipulados. Deve definir, também, o que é o e que não é permitido em termos de segurança, durante a operação de um dado sistema.” (Araújo, 2005, p. 19). A política de segurança de informação deve contemplar todos os esforços continuados, compreendendo os aspetos tecnológicos e humanos, para a proteção dos ativos da informação contra o risco de ocorrência de diversos tipos de ameaças, de forma a garantir a continuidade do negócio, minimizar os prejuízos, e contribuir para o alcanço dos objetivos da organização.

O nível de risco é potenciado pela amplitude da ameaça, pelas vulnerabilidades existentes e pelo impacto que possa causar no normal funcionamento da organização, mas pode ser reduzido em função das medidas de prevenção e segurança existentes. Uma política de segurança dos sistemas de informação tem como objetivo reduzir os riscos ao colocar em prática medidas de segurança que devem contemplar alguns aspetos básicos como sendo: a *prevenção*, a *deteção*, a *resposta* e a *recuperação*. Na ocorrência de um evento, a política de segurança deve também contemplar uma *análise*, de forma a retirar ensinamentos que permitam a sua melhoria contínua.

- *Prevenção*: o adágio popular “mais vale prevenir que remediar” resume a importância que a antecipação assume na gestão da segurança da informação. A prevenção tem como objetivo reduzir o risco de uma ameaça se concretizar, ao diminuir as vulnerabilidades do sistema. A prevenção de um incidente exige uma cuidada análise de risco e planeamento das ações de contenção e mitigação. A informação é um ativo que requer uma proteção proporcional ao seu valor, pelo que devem ser tomadas medidas de segurança para proteger as informações contra possíveis modificações, destruição ou divulgação não autorizadas, sejam acidentais ou intencionais. Durante a fase de prevenção, as políticas de segurança, os controles e os processos devem ser projetados e implementados. As políticas de segurança, os programas de sensibilização para a segurança e os procedimentos de controlo de acesso estão inter-relacionados e devem ser desenvolvidos desde o início. A política de segurança da informação é a pedra angular a partir da qual tudo mais é construído. Um dos componentes mais importantes numa política de prevenção é a redução dos riscos, sejam intencionais ou fortuitos, associados ao fator humano. Para tal, é

necessário formar e consciencializar os colaboradores para a importância e valor da informação e conseguir que colaborem de forma ativa, espontânea, consciente e comprometida na manutenção da segurança da informação (ISO/IEC 27002, 2013).

- *Deteção*: a constante monitorização de um sistema, que permita a deteção atempada de um ataque que possa comprometer o sistema, é de importância capital. Partindo do princípio que não há sistemas invioláveis, devem ser implementados sistemas de monitorização e de deteção de intrusões, ou intrusion detection systems (IDS), uma camada de segurança que, ao falhar de forma controlada devido a um ataque, desencadeia atempadamente uma notificação, permitindo a colocação em prática das contramedidas necessárias para responder à ameaça.
- *Resposta*: a resposta a um incidente de segurança deve ser cuidadosamente planeada, testada e ensaiada com bastante antecedência, de forma a evitar a tomada de decisões críticas ou improvisar respostas sob a pressão de um ataque. Os esforços, procedimentos e recursos devem ser proporcionais ao tipo de ameaça e descritos de forma clara num plano de resposta a incidente de segurança, que deve ser escrito e ratificado pelos níveis adequados da gestão. O plano de resposta deve priorizar claramente diferentes tipos de eventos e definir um nível de notificação ou resposta adequada ao nível do evento ou ameaça. Em alguns casos pode justificar-se a constituição de uma equipa de resposta a incidentes de segurança, cujas funções e responsabilidades específicas estejam claramente descritas.
- *Recuperação*: uma vez contida a ameaça, o sistema deve ser limpo e recuperado. Tal como o plano de resposta, o plano de recuperação deve estar claramente definido na organização. Este deve descrever as medidas, procedimentos e recursos necessários à reposição em pleno das funcionalidades do sistema, de forma a garantir a continuidade do negócio. A recuperação de um sistema pode passar pela reposição dos dados, aplicações, sistemas operativos ou de componentes físico do sistema. O plano de recuperação deve ser continuamente testado e validado, de forma a garantir a sua reposição em pleno, num espaço de tempo reduzido. Em alguns casos poderá justificar-se a utilização de sistemas redundantes ou de backup, que entrem em funcionamento, de forma manual ou automática, quando o sistema principal falha, de modo a minimizar o tempo de recuperação e o impacto na organização.
- *Análise*: após a ocorrência de um incidente, a colocação em prática das medidas adequadas, a contenção da ameaça e efetuada a recuperação do sistema, a

organização deve avaliar cuidadosamente os eventuais danos no sistema e levar a cabo uma análise detalhada sobre a ocorrência do incidente. Esta análise e relatório pós-incidente é o processo mais importante para o reforço do ciclo de segurança da informação, devido às lições aprendidas. Ao questionar quem, o quê, onde, porquê e quando e avaliando as suas respostas, a organização pode incorporar as lições aprendidas em cada uma das fases da gestão e do plano de segurança da informação.

2.4.5. Mecanismos de segurança

Com o objetivo de a garantir a confidencialidade, integridade e disponibilidade da informação, o sistema de segurança deve contemplar três eixos de atuação: a *prevenção*, a *deteção* e a *recuperação*. A Tabela 2.3, abaixo, sintetiza alguns dos mecanismos que poderão ser colocados em prática em cada uma dessas três vertentes.

Tabela 2.3: Mecanismos de segurança e controlo de ameaças
Fonte: baseado em Ribeiro (2007), ISO/IEC 27002 (2013) e Ribeiro (2016).

Prevenção	**Deteção**	**Recuperação**
• Controlo de acessos - Identificação - Autenticação - Autorização • Criptografia • Assinaturas digitais • Redundância de equipamentos • Sistemas de recuperação automática • Atualizações do sistema operativo • Atualizações das aplicações • Subscrição de listas CVE[2] • Utilização de antivírus e filtros de conteúdos • Codificação e normalização • Simulações e testes de penetração • Firewalls e VPNs • Protocolos seguros • Formação e sensibilização dos utilizadores • Planos de contingência e resposta	• Auditoria • Monitorização - Registos do sistema - Utilização do sistema - Atividades dos utilizadores - Erros de autenticação - Origem dos acessos e tentativas de acessos • Deteção de anomalias - padrões de comportamento - padrões de tráfego - ficheiros de aplicações e do sistema • Deteção de intrusões • Deteção de rootkits, trojans e outros códigos maliciosos • Deteção de ataques - negação de serviços - força bruta	• Cópias de segurança - diversos suportes - diversas localizações geográficas • Redundância hardware - Equipamentos - Componentes - Redes - Telecomunicações - Energia • Redundância software • Sistemas de recuperação automática • Mecanismos de restauro do sistema - snapshots - pontos de restauro • Recuperação de imagens do sistema • Reconstituição do sistema

2 https://cve.mitre.org

2.5. Computação na nuvem

Embora o termo se tenha popularizado nos anos mais recentes, o conceito de cloud computing (CC) ou computação na nuvem não é novo e, longo do tempo, foram surgindo diversas visões relacionadas com o tema. Com efeito, à medida que os computadores se foram tornando cada vez mais importantes e mais necessários, bem como foi aumentando a sua capacidade computacional, começaram também a ser investigadas novas técnicas que permitissem disponibilizar e partilhar esses recursos em larga escala e por diversos utilizadores. Abelson (1999) aponta John McCarthy como um dos percursores do conceito de cloud computing ao defender, numa palestra dada em 1961 no Massachusetts Institute of Technology (MIT), um novo paradigma de computação utilitária em sistemas de tempo partilhado, sob o qual, no futuro, a capacidade de computação poderia e deveria ser fornecida como um serviço público e comercializada como qualquer outro serviço, como os fornecimentos de água, eletricidade ou telefone. Em 1962, Kleinrock partilhava a sua visão de uma "Rede Galática" de computadores interligados onde qualquer pessoa pudesse aceder a dados e aplicações a partir de qualquer lugar (Leiner et al., 1999).

Em finais da década de 1960, Leonard Kleinrock previa que, embora as redes de computadores estivessem ainda na sua infância, à medida que crescessem e se tornassem mais sofisticadas, se iria generalizar o uso da computação utilitária nos escritórios e lares de todo o país, tal como os serviços de telefone e energia (Kleinrock, 2003). O mesmo autor partilha, em 2003, a sua visão da internet, assente em cinco características:

1. a tecnologia da internet será omnipresente;
2. estará sempre acessível;
3. estará sempre ligada;
4. qualquer pessoa poderá ligar-se a partir de qualquer lugar, com qualquer dispositivo e a qualquer hora; e
5. será transparente para o utilizador.

Na década de 1960, com a guerra fria no seu auge, a preocupação dos militares americanos era a criação de uma rede de telecomunicações não centralizada e que não pudesse ser destruída num ataque localizado. Em 1969 a Defense Advanced Research Projects Agency (DARPA) dava início à criação da Advanced Research Projects Agency Network (ARPANET), uma rede de utilização exclusivamente militar, baseada no conceito de

Kleinrock e na pesquisa de Paul Baran sobre a troca de pacotes de informação (Leiner et al., 1999). Com o desenvolvimento de novos protocolos de comunicação, nomeadamente o Transmission Control Protocol / Internet Protocol (TCP/IP), a ligação de diversos computadores em rede tornou-se uma realidade. A rede expandiu-se progressivamente e, com a ligação a algumas universidades, nos finais de 1969, a ARPANET contava com uma rede de quatro computadores interligados, lançando os fundamentos da atual internet (Kleinrock, 2003).

No entanto, o termo cloud computing, utilizado no contexto atual, parece ter sido popularizado por Eric Schmidt da Google, ao defender um novo modelo onde os serviços e arquitetura de residiriam algures na nuvem (Schmidt, 2006).

Os avanços tecnológicos verificados desde os anos 1960 e as melhorias nos serviços de fornecimento de acesso à internet abriram caminho ao aparecimento e à atual massificação da utilização da computação na nuvem. Em 1999, a Salesfore[3] disponibiliza o seu software de Costumer Relationship Manager (CRM) como um serviço disponível na internet e acessível diretamente a partir de um simples browser, num modelo de Software as a Service (SaaS), tornando-se pioneira na substituição de produtos físicos por serviços virtuais. Em 2006, a Amazon lança o Amazon Web Services (AWS)[4], um conjunto de serviços de computação na nuvem e acessíveis através da internet, que compreende, entre outros, o Amazon Elastic Compute Cloud (EC2), como plataforma de computação na nuvem, e o Amazon Simple Storage Service (S3), para armazenamento de dados. Também a Google, que já em 2004 tinha lançado o Google Mail, ou Gmail[5], um serviço de correio eletrónico, anuncia em 2006 o Google Docs[6], um pacote de aplicações de escritório com caráter fortemente colaborativo e utilização totalmente gratuita, compreendendo serviços de processamento de texto (Google Docs), folha de cálculo (Google Sheets), apresentações (Google Slides) posteriormente complementados com aplicações de gestão de inquéritos (Google Forms), diagramas (Google Drawings) e base de dados (Google Fusion Table) assente no seu serviço de armazenamento de dados (Google Drive).

Nos últimos anos tem-se verificado uma explosão nos fornecedores de serviços de cloud computing, não só por parte dos gigantes da informática, como a Microsoft (Microsoft

3 https://www.salesforce.com
4 https://aws.amazon.com
5 https://mail.google.com
6 https://docs.google.com

Azure[7]), a Google (Google Cloud Platform[8]), a Oracle (Oracle Cloud[9]) ou a IBM (IBM Cloud Services[10]), mas também startups que exploram nichos de mercado, como a Digital Ocean[11] ou a Linode[12], vocacionada para desenvolvedores.

Apesar de ser um tema tão popular atualmente, não existe uma definição unânime de cloud computing. De facto, Vaquero et al. (2008) contam 21 definições distintas para o termo cloud computing. No entanto, a que reúne mais consenso parece ser a publicada pelo National Institute of Standards and Technology (NIST).

De acordo com a definição do NIST, constante na sua Special Publication 800-145 de Setembro de 2011, o termo refere-se a um modelo que visa permitir, através da rede, o acesso ubíquo, conveniente e a pedido a um conjunto de recursos computacionais partilhados e configuráveis (como, por exemplo, redes, servidores, armazenamento de dados, aplicações e serviços) que podem ser rapidamente provisionados e lançados com um mínimo de esforço de gestão ou interação por parte do fornecedor de serviço (Mell & Grance, 2011).

Assim, a cloud pode ser considerada como um ambiente fiável e elástico onde todos esses recursos residem e a através da qual podem ser disponibilizadas os serviços pretendidos de acordo com os requisitos e as necessidades existentes num dado momento.

Ainda, segundo a definição do NIST, o modelo de nuvem é composto de cinco características essenciais, três tipos de serviço e quatro modelos de implantação.

De acordo com Mell e Grance (2011), as cinco caraterísticas essenciais do modelo são:

- *Acesso autónomo e a pedido*: o consumidor pode, unilateralmente, definir as capacidades de computação, como tempo do servidor e armazenamento em rede, de acordo com as suas necessidades e automaticamente, sem requerer interação humana com cada fornecedor de serviços.
- *Amplo acesso à rede*: as capacidades estão disponíveis na rede e são acessíveis por mecanismos estandardizados que permitem a sua utilização a partir de diversas plataformas clientes (por exemplo, smartphones, tablets, laptops e estações de trabalho) e localizações geográficas.

7 https://azure.microsoft.com
8 https://cloud.google.com
9 https://cloud.oracle.com
10 https://www.ibm.com/cloud-computing
11 https://www.digitalocean.com
12 https://www.linode.com

- *Agrupamento e partilha de recursos*: os recursos de computação do fornecedor são agrupados para atender múltiplos consumidores usando um modelo de coabitação, com diferentes recursos físicos e virtuais dinamicamente atribuídos de acordo com as necessidades do utilizador. Este não tem, geralmente, controle ou conhecimento da localização exata dos recursos que lhe são atribuídos, embora possa especificar a sua localização a um nível mais alto de abstração, como por exemplo, o país ou data center onde pretende o fornecimento dos serviços.
- *Elasticidade rápida*: as capacidades podem ser rapidamente provisionadas e liberadas, em alguns casos automaticamente, para escalar rapidamente e de forma proporcional às necessidades do momento. Do ponto de vista do cliente, as capacidades disponíveis parecem ser ilimitadas e podem ser apropriadas em qualquer quantidade a qualquer momento.
- *Serviço mensurável*. os sistemas em nuvem controlam e otimizam automaticamente a utilização de recursos, baseados na capacidade de medição a um nível de abstração apropriado ao tipo de serviço (por exemplo, armazenamento, processamento, largura de banda ou número de contas de utilizador ativas). Os recursos utilizados podem ser monitorizados, controlados e relatados, proporcionando transparência tanto para o fornecedor como para o consumidor do serviço utilizado.

O modelo de computação na nuvem constante na definição do NIST refere três modelos de serviços (Mell & Grance, 2011; Hashizume et al., 2013). Este conjunto é também designado como modelo SPI (SaaS, PaaS e IaaS) (Hashizume et al., 2013):

- *Infrastructure as a Service* (*IaaS*): neste modelo são fornecidos a capacidade de processamento, armazenamento, infraestruturas de rede e outros recursos de computação fundamentais, sobre os quais o cliente pode instalar e executar arbitrariamente diversos tipos de software, desde sistemas operativos a aplicações. Desta forma, o cliente não controla a infraestrutura física subjacente, mas tem controle sobre o sistema operativo, armazenamento e aplicações, e ainda algum controle sobre os componentes de rede. Estes recursos são disponibilizados sob a forma de máquinas virtuais ou espaços de armazenamento de dados instanciados pelo fornecedor de serviços e nas quais o utilizador pode, de forma autónoma, instalar e gerir sistemas operativos ou aplicações de acordo com as suas necessidades. Enquadram-se neste modelo de fornecimento de uma infraestrutura como serviço as

ofertas do Microsoft Azure, Amazon EC2, Google Compute Engine[13] (GCE), Digital Ocean ou o Linode.

- *Platform as a Service* (*PaaS*): neste modelo o fornecedor de serviços disponibiliza uma plataforma de desenvolvimento na nuvem constituída por uma infraestrutura completa e complementada com serviços, bibliotecas de programação, ferramentas de software e todos os demais componentes que possibilitam ao consumidor a implementação e alojamento de aplicações por ele desenvolvidas ou adquiridas. Entre os recursos disponibilizados encontram-se, tipicamente, sistemas operativos, bases de dados, linguagens de programação e servidores web. Embora toda a gestão da plataforma esteja sob a alçada do fornecedor de serviços, o cliente pode, normalmente, gerir alguns parâmetros dos componentes e do ambiente de desenvolvimento ou ainda escalar os recursos de forma elástica e automática. Neste modelo, ao libertar-se dos custos das complexas tarefas de gestão, configuração e manutenção da infraestrutura subjacente, o utilizador pode concentrar-se no desenvolvimento e gestão das suas aplicações. O Microsoft Azure e o Google App Engine são exemplos de plataformas disponibilizadas sob a forma de serviços.
- *Software as a Service* (*SaaS*): neste modelo, o fornecedor de serviços disponibiliza uma aplicação à qual o cliente pode aceder e utilizar através de uma interface web a partir de diversos dispositivos. Neste modelo, o cliente não gere nem controla a infraestrutura e plataforma subjacentes, mas pode personalizar certos aspetos específicos da aplicação, de forma a refletir as suas preferências ou necessidades. Desta forma, todas a tarefas de instalação, configuração, manutenção e suporte ficam a cargo do fornecedor. O serviço é fornecido ao cliente sob a forma de um custo fixo por cada utilização ou sob a forma de subscrição cujo preço pode variar de acordo com diversos critérios, tais como o número de utilizadores, as opções subscritas ou a fidelidade do cliente. Sendo um modelo extremamente popular, podem ser encontrados serviços tão diversos como o Google Mail (serviços de e-mail), Dropbox[14] (armazenamento de dados), Wordpress[15] (blogue), Microsoft Office 365[16] (ferramentas de escritório) ou o Salesforce (gestão de relacionamento com o cliente).

A Figura 2.4, abaixo, esquematiza as diferenças entre o modelo tradicional e o modelo SPI. Enquanto no primeiro, todos os componentes são geridos pelo cliente, nos modelos SPI

13 https://cloud.google.com/compute
14 https://www.dropbox.com
15 https://wordpress.com
16 https://login.microsoftonline.com

alguns componentes são fornecidos pelo fornecedor como um serviço (a sombreado), sendo complementados pelos componentes geridos pelo cliente.

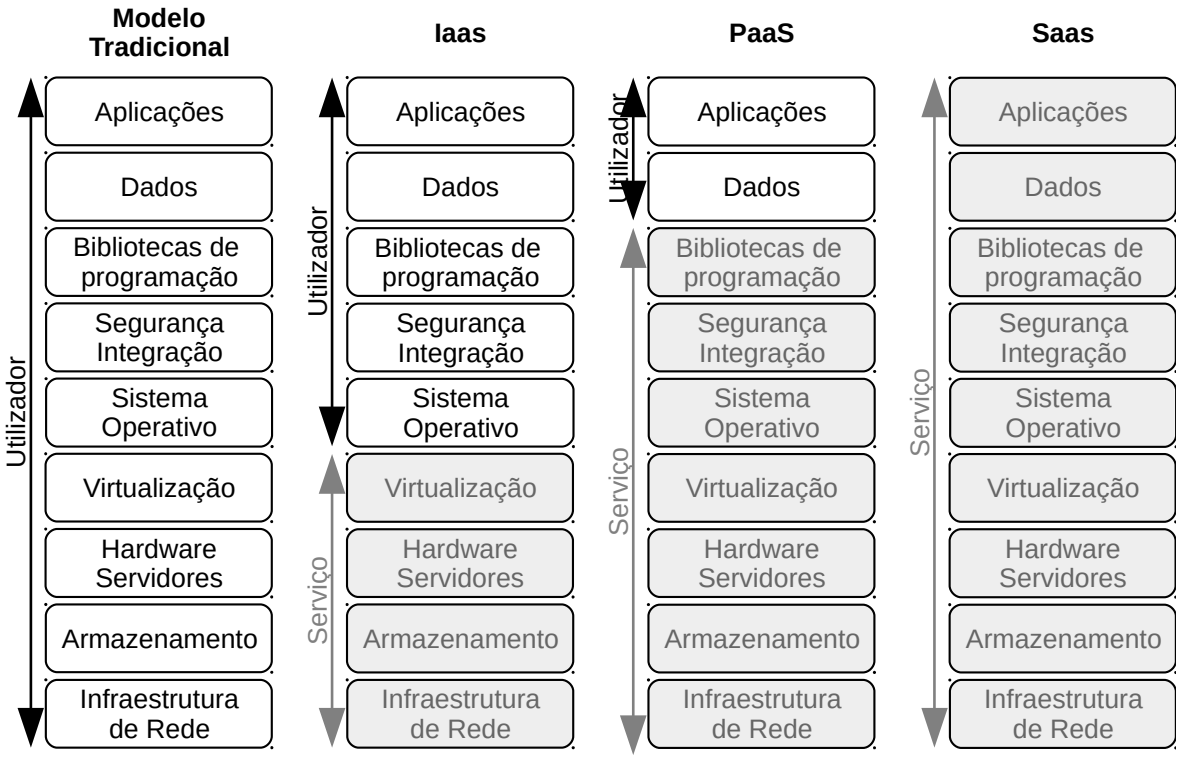


Figura 2.4: Comparação entre o modelo tradicional e o modelo SPI.
Fonte: baseado em Winkler (2011).

Ainda segundo Mell e Grance (2011), os quatro modelos de implantação são os seguintes:

- *Nuvem privada*: A infraestrutura da nuvem é de utilização exclusiva de uma organização, embora podendo compreender múltiplos consumidores ou unidades de negócio como, por exemplo, uma instituição bancária. Pode ser propriedade da organização ou fornecida por terceiros para uso exclusivo da organização, sendo gerida e operada pela organização, por terceiros ou de forma conjunta.
- *Nuvem comunitária*: A infraestrutura da nuvem é de utilização de uma comunidade específica de consumidores ou organizações com algum tipo de interesse comum como, por exemplo, uma rede de universidades. Pode ser propriedade de uma ou mais organizações da comunidade ou fornecida por terceiros para uso exclusivo da comunidade, gerida e operada por uma ou mais organizações da comunidade, por terceiros ou de alguma forma mista.
- *Nuvem pública*: A infraestrutura da nuvem é de utilização publica, podendo ser propriedade, gerida e operada por um fornecedor privado de serviços, organização académica ou governamental ou de forma conjunta.

- Nuvem híbrida: A infraestrutura da nuvem é composta por dois ou mais infraestruturas distintas que, mantendo as suas caraterísticas primárias, podem ser interligadas por algum tipo de tecnologia que permita a troca de dados ou de aplicações de forma normalizada.

2.6. Desafios da nomadicidade

Até meados da década de 1990 os computadores existiram sob a forma de equipamentos de grandes dimensões, instalados de forma praticamente inamovível num gabinete ou uma secretária e onde acesso à rede dependia da infraestrutura da organização para ligação aos seus servidores privados ou da existência de uma linha de comunicações fixa e dedicada para a ligação à internet. Gradualmente, os grandes sistemas foram dando lugar a computadores de secretária e estes a modelos com caraterísticas mais portáteis, ao mesmo tempo que os avanços nos serviços e equipamentos de telecomunicações e rede democratizaram o acesso à internet de tal forma que os utilizadores já não estão confinados a um local de trabalho fixo (Kleinrock, 2003).

Atualmente, o ato de viajar perdeu a sua condição de exceção e o nomadismo faz parte do nosso quotidiano, em que viajamos constantemente de casa para o escritório, do hotel para a sala de conferências, de carro, de comboio ou de avião, entre cidades, países ou continentes. Paralelamente, as dimensões cada vez mais reduzidas dos equipamentos, a sua crescente diversidade, autonomia e portabilidade, em conjunto com a gradual redução de custos e melhoria das infraestruturas de comunicação e acesso à internet transformaram os computadores, tablets e smartphones em utensílios pessoais de utilização constante.

O incontornável Leonard Kleinrock partilhava, em 2001, a sua visão do futuro da internet, onde os utilizadores acedem a rede não só a partir do ambiente de trabalho fixo da sua organização, mas adotam hábitos cada vez mais nómadas e passam a aceder, a qualquer momento, a uma rede de banda larga, cada vez mais omnipresente, onde quer que estejam, a partir de qualquer dispositivo, de forma simples e segura.

Esta “nomadicidade” é caraterizada por Kleinrock (2003) como o suporte do sistema necessário para fornecer capacidades e serviços de computação e comunicação aos nómadas, à medida que eles se movem de um lugar para outro, de forma transparente, integrada, convencional e adaptativa. Esta nomadicidade é conseguida aliando o uso de dispositivos portáteis de computação, como os laptops, tablets ou smartphones, às

tecnologias de comunicações móveis que possibilitam uma ligação à internet e tem como objetivo oferecer aos utilizadores uma experiência consistente em qualquer parte do mundo, incluindo quando e enquanto de deslocam de um local para outro. De facto, e ainda segundo o autor, o que distingue a utilização tradicional dos computadores desta nova condição de “nómada” é a enorme conetividade necessária.

Por ouro lado, os utilizadores nómadas, experimentam com frequência grande flutuações na qualidade e disponibilidade dessa conectividade, incluindo grandes períodos de comunicações a baixa velocidade ou ausência total de rede. Ciente destes obstáculos, o utilizador nómada desenvolve estratégias adaptativas mais ou menos elaboradas de forma a criar algumas garantias que as informações que possa necessitar estejam sempre disponíveis nos diversos dispositivos. Estas estratégias, passam, muitas vezes pela duplicação de ficheiros em vários dispositivos, tornando a gestão da informação extremamente complexa. Ainda, como consequência dessa duplicação de dados e informações, surge também a necessidade de gerir todas as aplicações e outros recursos necessários.

3. Estudo de caso

"Na preparação desta tournée, o meu manager falava-me de Nova Iorque, Rio de Janeiro, Londres, Berlim, Tóquio e… Tondela.
'Mas isso é a capital de quê?', perguntei-lhe eu, para obter uma resposta pronta:
'Não sei. Mas para estar aqui, é de certeza lugar de encontros...'
E estamos a ver isso mesmo, nesta capital de encontros!"

– Richard Bona, no seu primeiro concerto em Portugal, Tom de Festa 2007.
(Oliva, 2016)

3.1. Sobre a ACERT

A Associação Cultural e Recreativa de Tondela ou ACERT é uma organização não governamental, fundada em 1979, com sede em Tondela, e tem como objetivos a produção, promoção e divulgação de atividades culturais, artísticas, recreativas e desportivas, bem como a defesa do ambiente, que possam contribuir para o desenvolvimento regional, assim como para um salutar e benéfico aproveitamento e utilização dos tempos livres, desenvolvendo ainda, com carácter efetivo de continuidade, atividades de âmbito nacional, dirigidas a jovens.

Desde a sua génese, a ACERT definiu-se como "um projeto aberto à pluridisciplinaridade intercultural, assente numa prática não conformista nem complexada, como sinal das capacidades criativas e transformadoras […] e da importância de uma prática cultural, no desenvolvimento global e equilibrado das comunidades e das regiões." (ACERT, 2001, p. 20).

Apresentando-se como "o resultado das tensões, reflexão e debate entre quem com ela se identifica […] mas também das contradições, dificuldades e exigências que a renovação exige, numa prática e num projeto atuantes, coerentes e solidários" (ACERT, 2001, p. 20), a associação sempre demonstrou um caráter inclusivo, prática em que é correspondida, apoiada e acarinhada pela população local, sem nunca colocar de parte a sua vocação interventiva na sociedade, ao afirmar-se como "fazendo parte de um movimento nacional que, de uma forma independente, vem enriquecendo a vida cultural de Portugal" e onde as "relações desenvolvidas com outras associações, grupos e organizações, nacionais e internacionais, têm permitido um reaprender contínuo do significado da atuação solidária" (ACERT, 2001, p. 20).

Esta forma de ser e de estar da associação ACERT está em linha com o que é caraterizado por Herbert de Souza, quando sublinha a vocação política das ONGs, a importância do seu contributo para o desenvolvimento de uma sociedade alicerçada nos valores da democracia, liberdade, igualdade, diversidade, participação e solidariedade, apelidando-as de verdadeiros comités de cidadania impulsionadores da construção das sociedades democráticas sonhadas por todos (Souza, 1992).

A associação funciona, desde 1994, no espaço "Novo Ciclo ACERT", um antigo colégio convertido em espaço cultural multiusos que, segundo o protocolo entre a ACERT e a

Câmara Municipal de Tondela que lhe deu origem, pretende ser "[…] um espaço exemplar, pelos serviços culturais e comunitários que nele se irão realizar; um espaço de valorização concelhia de alcance regional, nacional e internacional [...]" (Oliva, 2016, p. 44).

O espaço Novo Ciclo ACERT contempla as seguintes infraestruturas: dois auditórios interiores, o primeiro com 276 lugares e o segundo com 116 lugares; uma galeria de exposições e sala de apoio; bar; oficina de artes gráficas e fotografia; estúdio de gravação áudio; estúdio de gravação e montagem vídeo; sala orgânica polivalente, onde ocorrem ensaios, espetáculos, gravações, dança, reuniões, formação, exposições; auditório ao ar-livre com 470 lugares, cabina técnica, proscénio avançado e cais de descarga; oficina de sonoplastia e iluminação; oficina de desenho gráfico; sala de reuniões; salas de formação; sala de produção; secretaria; loja cultural.

De acordo com os estatutos da associação, a sua direção, eleita para mandatos de dois anos, é composta por um presidente, um vice-presidente, um 1º secretário, um 2º secretário, um 1º tesoureiro, um 2º tesoureiro, e um número de vogais que pode variar entre os três, cinco, sete ou nove.

A associação é constituída por diversas secções ou núcleos de associados que, em campos de atividades específicos, visam a concretização dos objetivos gerais inscritos nos estatutos. Uma secção é constituída sempre que um conjunto de sócios que, em harmonia com os princípios estatutários e regulamentares, pretenda desenvolver trabalho num campo específico de atividades. As secções têm autonomia para eleger um corpo de responsáveis de coordenação, definir os seus objetivos e meios para os alcançar, poderão elaborar o seu próprio regulamento interno, desde que não contrariem Estatutos da Associação, o Plano de Atividades e o Orçamento da Direção, aprovados em Assembleia Geral. Todas as secções estão ainda dependentes da Tesouraria Central e obrigadas à apresentação regular de contas à Direção.

Atualmente, as diversas secções cobrem temáticas tão diversas como o Teatro, corporizado pelo grupo "Trigo Limpo Teatro ACERT", Cinema, Dança, Música, Novo Circo, Karaté, Basquetebol, Escalada, Programação do espaço Novo Ciclo até às secções de Formação e Educação, onde são promovidas, entre outras, aulas de inglês, representação ou ioga.

A ACERT considera também fundamental a colaboração com outras instituições e associações, quer a nível regional e nacional, quer a nível internacional. Esta colaboração manifesta-se de diferentes formas, desde o desenvolvimento de eventos e espetáculos em

parceria com outras associações, intercâmbios culturais internacionais, ou ainda na participação, muitas vezes com responsabilidades de coordenação, em redes colaborativas. Neste âmbito, a ACERT procura a integração em redes nacionais e internacionais de reflexão e ação sobre o tema "participação", tendo-se associado a diversas iniciativas ao longo dos seus quarenta anos de vida. Assim, a ACERT participou:

- de 2005 a 2008 na iniciativa comunitária "Equal", sob a epígrafe "Iguais num rural diferente", em parceria com a Associação para o Desenvolvimento Rural de Lafões (ADRL), o Instituto das Comunidades Educativas (ICE) e o Instituto Superior das Ciências do Trabalho e da Empresa (ISCTE);
- de 2012 a 2014 como coordenadora da rede portuguesa da Fundação Anna Lindh[17] para o diálogo intercultural, envolvendo 43 países da Europa e África Mediterrânica;
- de 2012 a 2014 no programa Time Case, integrado na iniciativa europeia Lifelong Learning Programme[18] (LLP) e atualmente integrado no programa Erasmus+;
- de 2015 a 2018 no European Academy of Participation[19] (EAP), integrado no programa Erasmus+ e que visa contribuir para uma Europa mais inclusiva, na qual as pessoas vivam juntas no respeito mútuo das suas diferenças.

Do ponto de vista funcional, as atividades desenvolvidas pela ACERT podem ser classificadas em três grandes categorias:

- *Serviços permanentes*, que asseguram o funcionamento quotidiano da associação e do espaço Novo Ciclo e dão suporte às atividades desenvolvidas pela associação e pelas suas diferentes secções. Encaixam nesta categoria os serviços de atendimento ao público, secretariado e contabilidade, serviços técnicos, serviços educativos, frente casa, programação cultural, marketing e comunicação ou ainda a direção artística.
- *Eventos recorrentes*, que ocorrem de forma cíclica e com uma periodicidade definida, com destaque para eventos como o FINTA – Festival Internacional de Teatro ACERT[20], o Tom de Festa – Festival de Músicas do Mundo ACERT[21] ou a Queima e Rebentamento do Judas[22]. Nesta categoria estão também as tarefas de administração e gestão que impõem uma ocorrência regular, como a produção e

17 http://www.annalindhfoundation.org
18 http://ec.europa.eu/education/lifelong-learning-programme_en
19 http://www.academyofparticipation.org/home
20 http://www.acert.pt/finta/2016
21 http://www.acert.pt/tomdefesta/2016
22 http://www.acert.pt/judas/2017

publicação da agenda trimestral, a elaboração do orçamento e plano de atividades anuais, relatórios de atividades e contas, reuniões da direção ou a realização das assembleias gerais ordinárias.

- *Projetos especiais*, englobando a ocorrência de projetos ou eventos pontuais e de natureza tão diversa como a preparação de uma exposição ou concerto, o lançamento de uma obra, a criação de uma peça teatral ou musical, a construção de uma máquina de cena ou a preparação de uma digressão. Produções ou coproduções como Valle Inclán Pirata, a construções de máquinas de cena como o Memoriar, o Pequeno Grande Polegar ou o Elefante Salomão são exemplos de projetos especiais. Nesta categoria estão também colaborações pontuais com outras associações ou organizações, bem como a venda ou compra de eventos especiais.

A gestão dos assuntos correntes da associação está a cargo de uma comissão de coordenação, mandatada pela direção e com a qual reúne periodicamente. Esta comissão de coordenação, composta por seis colaboradores permanentes da ACERT, tem como missão a concretização do Plano de Atividades e Orçamento em vigor.

De forma a assegurar os serviços permanentes, a organização procedeu também à criação de diferentes áreas funcionais, com competências específicas e prestando ou apoiando serviços específicos, de acordo com o organograma mostrado na Figura 3.1, abaixo.

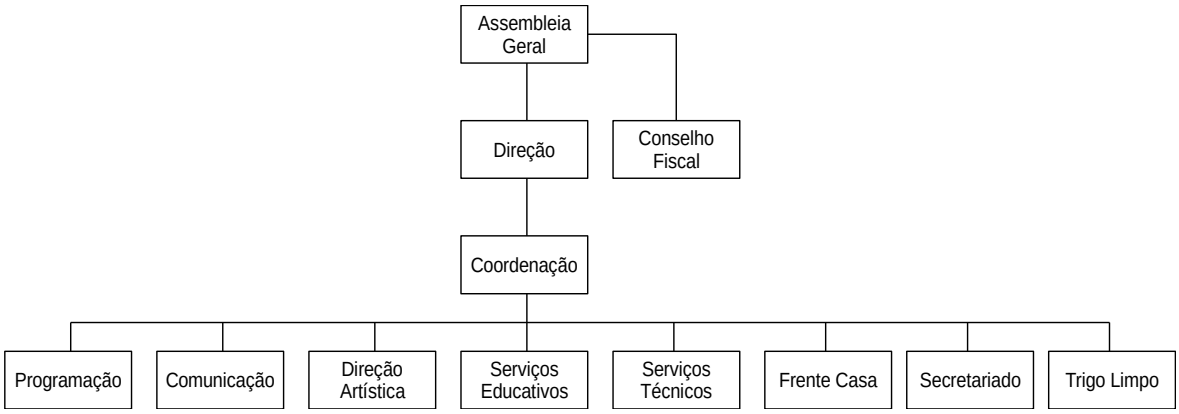


Figura 3.1: Organograma funcional da ACERT
Fonte: autor, baseado nas declarações dos entrevistados.

O funcionamento da organização é assegurado por um corpo de cerca de vinte colaboradores permanentes. Porém, em função das necessidades ditadas por alguns eventos recorrentes ou projetos especiais, o número de colaboradores pode aumentar temporariamente. Em algumas áreas, pela sua especificidade, ou porque não se verifica

uma necessidade real que justifique a criação de um serviço permanente, a organização recorre à contratação de serviços prestados por terceiros.

A cada uma das áreas funcionais identificadas estão afetos um conjunto de colaboradores. Estes, em função das suas competências e atribuições, poderão exercer em exclusividade numa área funcional ou, de forma transversal, colaborar noutras áreas funcionais. A Tabela 3.1, abaixo, ilustra essa distribuição dos colaboradores por áreas funcionais.

Tabela 3.1: Distribuição dos colaboradores por áreas funcionais na ACERT.
Fonte: autor, baseado nas declarações dos entrevistados.

Colaboradores	**Áreas Funcionais**									
	direção	**coordenação**	**programação**	**comunicação**	**direção artística**	**serviço educativo**	**serviços técnicos**	**frente casa**	**secretariado**	**trigo limpo**
Colaborador 01										●
Colaborador 02	●									
Colaborador 03	●									
Colaborador 04	●									
Colaborador 05						●				●
Colaborador 06	●									
Colaborador 07	●	●	●		●					●
Colaborador 08	●									
Colaborador 09	●		●							
Colaborador 10		●					●			
Colaborador 11	●		●					●		
Colaborador 12	●	●	●							
Colaborador 13									●	
Colaborador 14	●		●				●			
Colaborador 15										●
Colaborador 16	●	●			●					●
Colaborador 17		●				●				●
Colaborador 18	●		●							
Colaborador 19			●	●				●		
Colaborador 20									●	
Colaborador 21	●	●		●						

No entanto, esta distribuição não é totalmente estática, sendo bastante comum a reorganização temporária dos colaboradores em equipas virtuais, em função das necessidades ditadas pelos requisitos de um projeto ou evento. Esta forma de organização permite uma reatividade muito rápida e uma excelente adaptação às necessidades, dado que os participantes colaboram entre si numa relação de confiança, respeito e benefícios mútuos (Boavida e Ponte, 2002). Esta prática, facilita também a integração dos colaboradores mais novos, na medida em que proporciona e incentiva a aprendizagem e transferência de conhecimento tácito e boas práticas.

3.2. Metodologia

Neste estudo de caso procurou-se, numa primeira fase, compreender a problemática existente e as necessidades informacionais da organização. Sendo sobretudo um estudo exploratório, pretendeu-se recolher o máximo de informação possível, de forma cobrir os diversos aspetos do sujeito em estudo, pelo que se optou por recorrer a métodos de investigação qualitativos, nomeadamente entrevistas não estruturadas, observação direta e análise dos registos existentes (Fortin, 2009). Foram assim entrevistados cinco colaboradores, representando diversas áreas da organização, nomeadamente a Direção, Coordenação, Comunicação, Programação, Direção Artística, Frente Casa e Trigo Limpo. Desta forma foi possível estabelecer um retrato da organização, do modo como aquela geria a informação, das limitações existentes e das necessidades a colmatar.

No decorrer dos contactos preparatórios e das entrevistas aos colaboradores, foi possível constatar que nem sempre existia uma consciência clara sobre a importância da informação para a organização ou a necessidade da sua gestão e segurança. Assim, de forma a sensibilizar os colaboradores para a importância da informação e da sua segurança foram organizadas ações de sensibilização, sob a forma de workshops, onde, numa primeira fase, se demonstrava a importância da informação para a organização, a necessidade e as vantagens da sua gestão e segurança e, em seguida, se promoveu o debate convidando os participantes a partilharem a sua experiência e formularem conclusões e lições a reter. Os dois workshops já realizados, pela sua interatividade e debate de ideias, constituíram um espaço de reflexão e consciencialização muito importantes para os colaboradores, o que proporcionou uma intervenção mais informada na definição das necessidades e ambições para o plano de gestão da informação. Estes workshops, com uma duração aproximada de

duas horas, decorrem em quatro fases: inicialmente, o tema é introduzido pelo animador recorrendo a uma pequena apresentação; em seguida é promovida a discussão do tema e a partilha de experiências e casos reais na primeira pessoa; numa terceira fase, os participantes são convidados a escrever até três regras ou boas práticas relacionadas com o tema em debate; finalmente, as sugestões dos participantes são recolhidas e debatidas, sendo, no final, sintetizadas num documento aprovado pelos participantes.

De forma a proporcionar uma clara compreensão das necessidades reais dos utilizadores, estes foram envolvidos, desde o início, na definição dos requisitos do plano de organização e gestão da informação (Choo, 2003). Esta abordagem proporcionou não só a possibilidade de conceber um plano de gestão da informação adequado à organização e ao seu modelo de negócio, como também facilitou a assimilação e adoção do plano pelos utilizadores, permitindo a sua integração nas rotinas de trabalho quotidianas de forma não disruptiva e bastante natural.

Na elaboração do plano de classificação e segurança da informação, bem como da estrutura de organização da informação e hierarquia de pastas que a suporta, foi tido em conta o modelo de negócio e as necessidades da organização, para além de se colocar especial cuidado na designação das classes, tendo-se procurado utilizar temos familiares para os utilizadores, com o objetivo de facilitar a compreensão e o significado das diversas categorias e de que forma estas se relacionam umas com as outras (Krippendorff, 1973). Para o estabelecimento do plano de classificação da informação procedeu-se, em primeiro lugar à identificação das funções e atividades desenvolvida pela organização e, em seguida, ao seu agrupamento em conjuntos lógicos de atributos comuns (Mas, 2007).

Como suporte ao plano de classificação, segurança e gestão da informação, foi também elaborado um conjunto de documentação de sensibilização e informação, bem como manuais de utilização, boas práticas e regras detalhadas, definindo não só como a informação deve ser manipulada na organização, mas também estipulando claramente os limites e obrigações nas operações de gestão da informação, de forma a garantir a segurança da informação (Araújo, 2005).

O sistema de gestão da informação foi posteriormente implementado numa aplicação alojada num servidor na nuvem. De forma a que o impacto da adoção do sistema de gestão da informação pela organização seja minimizado, a sua implementação está a decorrer de forma faseada. O projeto prevê assim três fases principais, sendo a primeira de preparação

de uma prova de conceito, a segunda de arranque limitado a um grupo piloto restrito e, posteriormente, o alargamento a toda a organização. Esta abordagem permite testar a soluções, analisar os resultados e introduzir as eventuais correções necessárias num ambiente controlado, de forma a que, na fase de alargamento a toda a organização, não só terá um maior nível de maturidade e estabilidade, representando uma prova de conceito funcional, como também permitirá a partilha de conhecimento tácito e explícito entre os utilizadores, o que irá facilitar a sua adoção.

3.3. Problemática

Anteriormente à intervenção realizada no âmbito deste estudo, não existia na ACERT qualquer política concreta de organização da informação. Os utilizadores privilegiavam, em função das sua experiência e competência, um esquema de classificação muito pessoal, procurando dar resposta às suas necessidades quotidianas mais imediatas, em detrimento de uma visão mais institucional e cooperativa (Mas, 2007). A perspetiva vigente era, na prática, a necessidade de proceder ao armazenamento de ficheiros de forma a satisfazer as necessidades ditadas pelas suas tarefas individuais ou do grupo restrito que que o utilizador esteja inserido, em detrimento de uma verdadeira política global e sistemática de gestão da informação a nível da organização.

3.3.1. Armazenamento de ficheiros

A informação da organização encontrava-se alojada, de forma bastante dispersa, em três tipos de sistemas distintos:

- No computador de cada utilizador, sendo as principais justificações para esta prática a facilidade de acesso (tendo informação no computador portátil é possível trabalhar em qualquer lugar) ou a crença que mais ninguém necessita daquela informação (arquivo de mensagens de correio eletrónico). Na maioria dos casos estudados, não eram efetuadas cópias de segurança com regularidade, o que coloca em risco toda a informação em caso de falha ou ataque informático. Desta prática resulta também o efeito perverso em que, na ausência do utilizador, e de modo a que outros possam aceder à informação, as suas credenciais de acesso são as mesmas para diferentes sistemas e do conhecimento dos restantes colaboradores.

- Numa pasta partilhada no servidor de ficheiros, apenas acessível na rede interna, e onde reside informação diversa, sem uma organização formal e sem um controlo de acessos efetivo. Esta prática coloca em risco os três pilares da segurança da informação (Beal, 2005; Peixoto, 2006): a confidencialidade (é possível aceder, da mesma forma, a informação pessoal dos utilizadores e a informação confidencial da organização), a integridade (qualquer utilizador não autorizado pode alterar a informação) e a disponibilidade (é possível, de forma intencional ou fortuita, eliminar qualquer documento ou hierarquia de pastas) e coloca em causa também caraterísticas tão fundamentais como a autenticidade e o não repúdio (Camp, 2001; Adachi, 2004;) ou mesmo a própria legalidade da informação (Sêmola, 2003).
- Em serviços de armazenamento externos, como a Dropbox[23], opção justificada pela necessidade de partilhar informação e ficheiros com parceiros e fornecedores externos. Dada a limitação de espaço de armazenamento destes serviços, os utilizadores trabalham a informação nos seus sistemas pessoais e, na fase final do seu trabalho, depositam os ficheiros numa pasta da Dropbox, onde os parceiros poderão recuperar ou alterar a informação. No entanto, são obrigados a apagar, previamente, ficheiros mais antigos de forma gerar espaço de armazenamento para os novos ficheiros. Desta prática resultam a duplicação da informação, a dúvida sobre qual a informação válida e original e o risco de perda de informação durante as operações de eliminação de ficheiros para criação de espaço de armazenamento.

3.3.2. A perspetiva dos utilizadores

A conceção e implementação de um sistema de gestão da informação deve basear-se numa clara compreensão das verdadeiras necessidades de informação dos utilizadores (Choo, 2003). Desta forma, foram organizadas diversas entrevistas, aos elementos da direção e aos colaboradores dos diversos núcleos da instituição. Durante as entrevistas, conduzidas de forma não estruturada e informal, os utilizadores demonstraram estar conscientes de algumas das limitações na forma como a informação era gerida e organizada, manifestaram algumas preocupações relativamente à sua segurança e identificaram algumas lacunas e necessidades associadas à forma como a informação é pesquisada, partilhada e acedida.

O relato de um colaborador da frente casa, referindo-se ao processo de reserva e venda de bilhetes, demonstra as dificuldades existentes: “Nós temos um número de telefone para

23 https://www.dropbox.com

efetuar reservas e uma folha excel no servidor interno onde as anotamos, mas muitos espetadores ligam diretamente para o meu telemóvel. Nesse caso, eu anoto a reserva e quando chego à ACERT atualizo a folha de reservas. O problema é que eu não tenho forma de saber se realmente ainda há lugares ou se o evento já está esgotado, e aconteceu algumas vezes espetadores ficarem sem lugar que tinham reservado".

As principais preocupações e necessidades manifestadas pelos utilizadores, bem como as constatadas por observação direta e resultantes da análise dos dados existente, foram organizadas em quatro categorias principais, identificadas e exemplificadas abaixo:

- Organização da informação:
  - Não existe uma uniformização na organização da informação o que dificulta a sua recuperação, particularmente na informação partilhada.
  - Cada utilizador cria o seu próprio esquema de organização e hierarquia de pastas, nem sempre de acordo com as necessidades do grupo e nem sempre compreendida ou subscrita pelos outros utilizadores.
  - Os nomes das pastas nem sempre são claros, nem sempre refletem o seu conteúdo, e muitas vezes os termos são repetidos nas diversas pastas e subpastas.
  - A mesma informação pode estar repetida em diferentes pastas, dificultando a sua pesquisa, recuperação e suscitando dúvidas sobre qual é o original ou a versão mais recente.
  - Não existe uma diferenciação ou classificação que defina o âmbito da distribuição da informação ou limite a divulgação de informação sensível ou estratégica para a organização.
- Pesquisa da informação:
  - Não existe nenhuma ferramenta que possibilite a pesquisa pelo nome do ficheiro, nem pelo seu conteúdo, nem pelos seus metadados.
  - A pesquisa é feita manualmente, navegando pelas pastas e ficheiros, por tentativa e erro, frequentemente em diferentes sistemas, resultando num processo moroso e, muitas vezes, infrutífero.
  - Não existe forma centralizada e uniformizada de pesquisar diversos tipos de informação, como documentos de texto, folhas de cálculo, imagens, mensagens correio eletrónico, listas de tarefas, eventos agendados ou endereços de correio eletrónico, sendo necessário recorrer a diversas aplicações específicas;

- Partilha da informação:
  - Não existe um método de partilhar a informação internamente, com colegas ou grupos de trabalho, de forma controlada.
  - A partilha de informação com colegas ou grupos internos é efetuada de forma indiferenciada, depositando os documentos numa pasta partilhada, de acesso livre e sem qualquer restrição, para toda a organização;
  - Não existe um método fácil de partilhar a informação com parceiros externos, sendo necessário recorrer à Dropbox;
  - A partilha de informação com parceiros externos é efetuada recorrendo à Dropbox;
  - A Dropbox tem uma capacidade de armazenamento bastante limitada, obrigando o utilizador a apagar ficheiros antigos antes de carregar os novos;
  - O processo de partilha recorrendo à Dropbox é muito complexo, moroso e pode originar perda de informação: é necessário copiar ficheiros antigos para uma pasta do servidor interno, apagar os ficheiros na Dropbox, carregar os ficheiros a partilhar e, caso o parceiro crie ou alter ficheiros, é também necessário descarregar ou sincronizar os ficheiros com o sistema local e ou com o servidor interno.
- Acesso à informação em mobilidade:
  - Não é possível aceder ao servidor interno a partir do exterior (o acesso está limitado à rede interna).
  - Para aceder à informação a partir do exterior é necessário, previamente, copiar os ficheiros para a Dropbox.
  - É muito difícil ou mesmo impossível aceder à informação a partir de dispositivos como o tablet ou o smartphone.
  - Não existe forma integrada e unificada de usufruir de determinados serviços, como agenda, calendário, videoconferências, ferramentas de organização e gestão ou outras ferramentas colaborativas sem ser necessário recorrer a serviços externos e a aplicações com custos de instalação e utilização.

3.4. Organização da informação

De forma a responder às necessidades detetadas e às preocupações demonstradas pela organização, foi definido uma estratégia de organização da informação baseado em quatro eixos principais:

6. a criação de um plano de classificação para a informação;
7. a criação de uma estrutura de pastas e ficheiros de suporte a esse plano;
8. a criação de uma plataforma informática de gestão da informação; e
9. a criação de um plano de formação e sensibilização dos utilizadores.

3.4.1. Classificação da informação

Para estabelecer um plano de classificação da informação procedeu-se, em primeiro ligar à identificação das funções e atividades desenvolvida pela organização e, em seguida, ao seu agrupamento em conjuntos lógicos de atributos comuns (Mas, 2007), com base na análise do organograma da Figura 3.1, acima, nas entrevistas aos colaboradores, na observação direta e na análise dos dados existentes.

Na conceção desta classificação, trabalhada em conjunto com os coordenadores da organização, procurou-se definir uma estrutura que reflita e seja adequada ao modelo de negócio da organização, tentando manter, ao mesmo tempo, a sua simplicidade e clareza. Assim, foi usada uma abordagem do geral para o particular, optando-se por um plano de classificação orgânico-funcional, tendo como classe principal o nome da unidade orgânica identificada no organograma da organização. Ao refletir as atividades da organização na estrutura da classificação pretendeu-se facilitar os processos de pesquisa e recuperação da informação, dado o conhecimento que os utilizadores detêm da organização (Collet, 2012).

Desta forma e seguindo as recomendações da norma ISO 15489:2016, onde é defendido que o nível superior da classificação deve descrever as principais funções da organização, foram definidas as classes “Direção”, “Coordenação”, “Programação”, “Comunicação”, “Direção Artística”, “Serviços Educativos”, “Serviços Técnicos”, “Frente Casa”, “Secretariado” e “Trigo Limpo”.

No segundo nível da classificação foram tidas em conta a tipologia das atividades e funções principais desenvolvidas por cada grupo orgânico. Identificaram-se neste nível dois conjuntos de atividades: um primeiro, transversal a todas as unidades organizacionais

e um segundo, específico às funções especializadas desenvolvidas por cada unidade. Neste nível, foram criadas, de forma transversal, as classes “Eventos Recorrentes” referente a eventos que ocorrem de forma cíclica e repetitiva, “Projetos Especiais” albergando informação referente a eventos pontuais e não repetitivos, e “Documentação Corrente” contendo documentação de utilização permanente e quotidiana. Complementarmente, foram também criadas classes específicas referentes às atividades desenvolvidas de forma especializada por cada unidade orgânica.

O terceiro nível e seguintes tornam-se cada vez mais específicos e foram objeto de análise e definição caso a caso, procurando a microestrutura adotada refletir as caraterísticas do evento, projeto ou assunto descrito (ISO 15489, 2016). Assim, dentro das classes de primeiro e segundo nível “Comunicação” e “Eventos” poderemos encontrar as classes e as subclasses “Festivais” e “Teatro”, refletindo a tipologia do evento e ainda as subclasses “Finta” e “2017”, referentes ao nome e edição do evento regular.

A profundidade do esquema de classificação da informação adotado tem uma média de quatro a cinco níveis. Desta forma, pretende-se facilitar a pesquisa, armazenamento e recuperação da informação e, ao mesmo tempo, permitir uma adoção mais rápida pelos utilizadores que tem à sua disposição um modelo que lhes é familiar, intuitivo e de fácil assimilação, compreensão e atualização.

3.4.2. Organização e estrutura das pastas

Na conceção do esquema de organização das pastas dentro do repositório, foram tidas em conta as necessidades ligadas ao modelo de negócio da organização e o modo como a informação será utilizada pelos seus membros, de forma a facilitar a partilha e recuperação da informação (Choo, 2003). A conceção desde esquema de organização ocorreu em duas fases: numa primeira parte analisou-se a estrutura funcional da organização de forma caraterizar e determinar as diferentes classes utilizadas e, numa segunda fase, dedicou-se especial cuidado à escolha da notação a utilizar, tendo sido adotados termos claros, coerentes, significativos e familiares para o utilizador (Mas, 2007).

A estrutura adotada é constituída por uma hierarquia principal de três níveis, sendo que o primeiro reflete a unidade orgânica, o segundo nível identifica o tipo de atividade desenvolvida e o terceiro e seguintes estão associados ao processo ou tarefa no âmbito da qual se produziu ou adquiriu a informação. Embora parta de uma base comum, esta

estrutura é suficientemente flexível e hospitaleira para permitir ao utilizador alguma latitude na ampliação da estrutura existente, em função das suas necessidades ou das necessidades da sua unidade organizacional.

Com base nestas premissas, foram definidos o seguinte conjunto de diretrizes e boas práticas para a criação ou extensão da hierarquia de pastas.

- Os nomes das pastas e ficheiros deverão respeitar as regras de nomeação de pastas e ficheiros definidos no manual de boas práticas para a nomeação de ficheiros.
- Os nomes das pastas deverão ser claros, coerentes, relevantes e ilustrativos das categorias que representam.
- Sempre que possível, os nomes das pastas deverão ser normalizados e transversais às diversas unidades funcionais, de forma a facilitar a organização, pesquisa e recuperação da informação.
- A profundidade da hierarquia deve ser apenas a mínima necessária, evitando a criação de um excessivo número de subpastas, por forma a facilitar a legibilidade, navegação, pesquisa e recuperação da informação.

Complementarmente, e de forma a uniformizar a estrutura definida, facilitar a partilha entre grupos e fomentar a utilização do esquema de classificação e organização da informação, foi também determinado um conjunto de regras a seguir pelos utilizadores.

1. Cada unidade funcional dispõe de uma pasta no topo da hierarquia do repositório, correspondente ao primeiro nível da classificação adotada e identificada pelo nome da unidade funcional, desprovido de caracteres especiais, de forma garantir a compatibilidade entre os diversos dispositivos e sistemas operativos. Esta pasta será partilhada, com direitos de leitura e escrita, por todos os membros dessa unidade funcional. No primeiro nível foram criadas as pastas “`Acert`”, “`Basquetebol`”, “`Comunicacao`”, “`Coordenacao`”, “`Direcao`”, “`Escalada`”, “`Programacao`”, “`Secretariado`”, “`ServicoEducativo`”, “`ServicoTecnico`” e “`TrigoLimpo`”.
2. Num segundo nível, deverão existir, obrigatoriamente, as seguintes pastas:
   a. `10_Eventos`: Informação relativa a eventos recorrentes;
   b. `20_Projetos`: Informação relativa a projetos e eventos não recorrentes;
   c. `30_Documentos`: Informação utilizada regulamente pelos serviços permanentes e necessária para o desempenho das tarefas quotidianas do serviço;

d. `90_Partilhas`: Informação partilhada dentro da organização (entre grupos) ou fora da organização (com parceiros externos);

e. `95_Outros`: Informação não classificável nas categorias existentes. O conteúdo desta pasta poderá ser indicador da necessidade de criação de novas categorias ou subcategorias que permitam a correta classificação desta informação (Mas, 2001).

f. `99_Arquivo`: Informação em fase não ativa ou que deva respeitar um período de arquivo antes da sua destruição, de acordo com a política de retenção (Krippendorff, 1973). A estrutura deverá reproduzir, a partir desta pasta, a hierarquia de segundo nível.

Em função das necessidades específicas de cada unidade funcional, poderão ser criadas outras pastas, que deverão respeitar classificação e a nomenclatura indicada.

3. No terceiro nível e seguintes deverão ser criadas pastas e subpastas da forma que melhor ilustre cada um dos processos ou objetivos a realizar dentro da categoria representada pelo segundo nível e alinhadas com o plano de classificação da informação.

   a. `10_Eventos`: Pasta e subpastas com o tipo e subtipo de evento, nome e periodicidade de ocorrência.

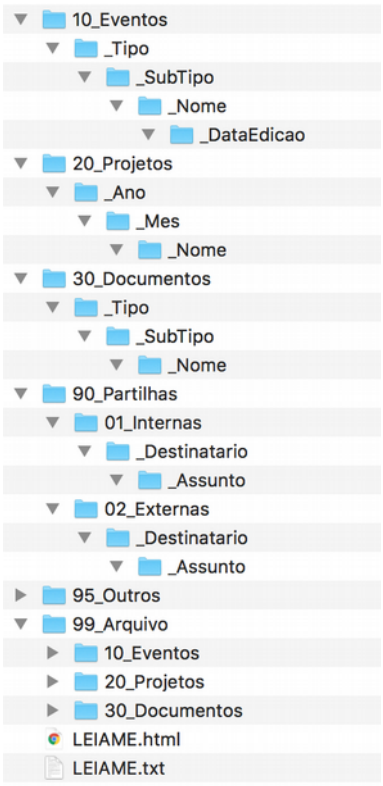
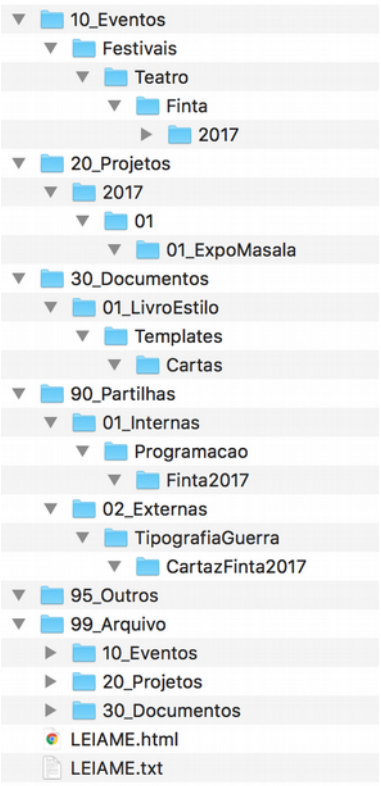
   b. `20_Projetos`: Pasta e subpastas com a data e nome do projeto.

   c. `30_Documentos`: Pasta e subpastas representativas da tipologia documental. Poderão ser complementadas com outros elementos identificativos relevantes.

   d. `90_Partilhas`: Pastas e subpastas representativas do tipo de partilha (interna ou externa), destinatário e assunto. Estas partilhas devem ter sempre um caráter temporário e limitado no tempo.

Esta estrutura hierárquica de pastas e ficheiros é ilustrada na Tabela 3.2, abaixo.

Tabela 3.2: Exemplo de utilização da hierarquia de pastas.
Fonte: autor.

Abstração da hierarquia das pastas	Aplicação na unidade funcional "Comunicação"
	

Deste conjunto de diretrizes e regras de utilização da hierarquia de pastas e ficheiros resultou um manual detalhado de regras e boas práticas para a sua utilização quotidiana, enriquecido com diversos exemplos ilustrativos da sua aplicação prática.

3.4.3. Plataforma colaborativa de gestão da informação

A plataforma colaborativa de gestão de informação deveria responder à necessidades dos utilizadores e ser, ao mesmo tempo, não intrusiva e de fácil utilização. Em conjunto com a coordenação, estabeleceu-se que a plataforma deveria cumprir os seguintes requisitos, considerados como essenciais pela organização:

- Constituir um ponto de acesso unificado para todo o sistema de gestão da informação;
- Ser de utilização fácil e intuitiva, com uma curva de aprendizagem reduzida;
- Permitir o acesso, de forma transparente, a partir da rede interna e da internet;
- Permitir o acesso a partir de vários dispositivos e sistemas operativos;
- Ser utilizável, na sua plenitude, a partir de uma interface web;

- Permitir a partilha de ficheiros internamente e com parceiros externos, de forma controlada e segura;
- Possibilitar a integração com os equipamentos e softwares existentes;
- Permitir a gestão de acessos e organização em grupos de colaboração;
- Proporcionar resultados de pesquisas baseadas no nome, conteúdo e metadados dos ficheiros;
- Permitir a gestão de diversas tipologias documentais (textos, imagens, endereços, correio eletrónico, registos vídeo e áudio);
- Permitir a visualização e edição dos ficheiros sem necessidade de os descarregar ou de instalar software específico;
- Proporcionar ferramentas colaborativas, nomeadamente a edição simultânea de documentos;
- Proporcionar ferramentas de comunicação, nomeadamente de troca de mensagens de texto e videoconferência;
- Ser baseada em normas abertas de forma a facilitar a integração com aplicações futuras e página web da associação;
- Permitir a migração da informação existente para a nova plataforma;
- Proporcionar um baixo custo de utilização.

Se bem que existindo atualmente várias ofertas de serviços na área de armazenamento de ficheiros e gestão da informação estas foram excluídas por não cumprirem todos os requisitos. Os principais fatores que levaram à exclusão destas ofertas foram:

- As ofertas “gratuitas” são muito limitadas no espaço de armazenamento oferecido;
- Algum dos requisitos só estão disponíveis nas versões “premium” ou empresariais, com elevados custos de subscrição e utilização;
- A eventual integração de vários serviços com o objetivo de cumprir todos os requisitos reveste-se de uma complexidade de implementação e utilização que torna a solução inviável;
- O custo de aquisição de armazenamento ou funcionalidades extra, de forma a cumprir com os requisitos, torna-as proibitivas para o orçamento definido pela organização;

Assim, a aplicação que permitiu cumprir todos os requisitos foi a Nextcloud[24]. Esta é uma aplicação de código aberto que, na sua configuração de base, permite o fornecimento de serviços de armazenamento e partilha de ficheiros, de forma bastante semelhante à Dropbox. No entanto, a sua arquitetura modular possibilita a extensão das suas funcionalidades recorrendo à instalação de diversas "app" disponibilizadas a partir da sua "appstore"[25] que, uma vez instaladas, funcionam e são apresentadas ao utilizador como se de uma aplicação única se tratasse.

Esta aplicação foi instalada num servidor virtual privado (VPS) alojado na DigitalOcean, num fornecedor de infraestrutura como serviço (IaaS), num dos seus data centers localizado na Europa. O servidor virtual privado tem como base o sistema operativo Linux[26], fornecido pela distribuição Debian[27], versão 8 "Jessie" e um conjunto de aplicações que viabilizam um servidor web vulgarmente conhecido por LEMP, um acrónimo para Linux (sistema operativo), Nginx[28] (servidor web), MariaDB[29] (servidor de base de dados) e PHP[30] (linguagem de programação) e sobre esta plataforma instalou-se a aplicação Nextcloud.

A configuração atual, constituída por uma máquina virtual com processador de 2 núcleos, memória de 2Gb e um disco de estado sólido (SSD) de 40Gb, que é complementado com um espaço de armazenamento dedicado de 100Gb, podendo ser expandida de forma elástica a qualquer momento, em função das necessidades. A nuvem privada (Mell e Grance, 2011) assim constituída, utiliza um subdomínio da organização e está disponível no endereço https://cloud.acert.pt.

Dado que toda a solução utiliza aplicações de código aberto e utilização livre, eliminou-se a necessidade de aquisição de licenças, o que limitou os custos aos valores da subscrição dos serviços de computação, espaço de armazenamento e cópias de segurança, o que se traduz num encargo aproximado de € 34 mensais ou € 400 anuais para a associação.

A Tabela 3.3, abaixo, demonstra, em detalhe, os custos mensais e anuais da solução, em dólares dos Estados Unidos.

24 https://nextcloud.com
25 https://apps.nextcloud.com
26 https://www.linux.org
27 https://www.debian.org
28 https://nginx.org
29 https://mariadb.org
30 https://secure.php.net

Tabela 3.3: Detalhe dos custos da solução.
Fonte: autor.

Designação do serviço	Custo mensal	Custo anual
Virtual Private Server (2GB / 2CPU / 40GB SSD)	$ 20.00	$ 240.00
Droplet backup	$ 4.00	$ 48.00
Block Storage (100GB)	$ 10.00	$ 120.00
Off site backup	$ 3.00	$ 36.00
Total	**$ 37.00**	**$ 444.00**

Uma vez instalada e configurada a aplicação, para além de cumprir todos os requisitos definidos pela ACERT e pelo plano de organização e classificação da informação adotado, fornece ainda os seguintes serviços e opções:

- Sincronização de ficheiros em tempo real com os principais sistemas operativos para computadores de secretária ou portáteis, tablets e smartphones;
- Agenda, calendário, listas de tarefas e gestão de contactos compatíveis com as principais aplicações de correio eletrónico e agendas;
- Sincronização de mensagens telefónicas SMS;
- Edição colaborativa de ficheiro de texto, folhas de cálculo ou apresentações, graças à integração do LibreOffice Online[31];
- Aplicação de gestão de projetos online;
- Cliente de correio eletrónico, permitindo agregar e apresentar diversas contas numa única interface;
- Aplicação de áudio e videoconferência, com possibilidade de partilha do ecrã;
- Criação de “círculos” ou equipas de trabalho virtuais, de forma a facilitar a comunicação e colaboração;
- Partilha segura de ficheiros com parceiros externos, de forma pública ou privada, permitindo o download e o upload de ficheiros de forma controlada;
- Integração de serviços externos de armazenamento na nuvem, como o Google Drive, Dropbox ou o Microsoft Sharepoint[32].
- Integração como outros servidores Nextcloud, possibilitando a constituição de uma federação de servidores ou nuvem mista.

31 https://www.collaboraoffice.com/code
32 https://products.office.com/en-us/sharepoint

O Nextcloud fornece também algumas opções orientadas especificamente para a gestão e organização da informação, nomeadamente:

- Gestão automatizada de versões de ficheiros e histórico das alterações;
- Adição de metadados sob a forma de etiquetas, atribuídas manualmente ou de forma automática, mediante regras definidas pelos utilizadores;
- Política de retenção de ficheiros, personalizável mediante regras definidas pelos utilizadores;
- Registo de eventos, transversal a todo o tipo de informação, detalhando dados como o utilizador e o tipo de operação efetuada;
- Ferramenta avançada de pesquisa, transversal a toda a informação alojada no servidor, capaz de devolver resultados a partir dos nomes dos ficheiros e seus conteúdos, metadados associados a textos, imagens vídeos ou áudio, bem como resultados da agenda, calendário, contacto e mensagens SMS;

3.4.4. Segurança da informação

Especial cuidado foi colocado na gestão da segurança da aplicação e do servidor. Dado que, das três camadas de segurança da informação (Sêmola, 2003; Araújo, 2005), a camada física é assegurada pelo fornecedor da plataforma, foram trabalhadas a componente humana, por via de ações de sensibilização e formação e a componente tecnológica, ao colocar em prática diversas estratégias de segurança do sistema e da informação.

A segurança foi facilitada pelo facto de a aplicação Nextcloud cumprir as especificações da norma ISO/IEC 27001 (2013) para a gestão de segurança da informação e o seu código fonte ser regularmente auditado por organizações independentes[33]. Como complemento, foram ainda colocados em prática diversas medidas de proteção, deteção e resposta, nomeadamente:

- *Proteção*: firewall permitido apenas ligações seguras ao servidor; acesso condicionado à utilização de protocolos seguros (https e ssh); utilização de certificados digitais; política forçada de passwords seguras; passwords únicas e diferenciadas para cada aplicação ou dispositivo cliente; autenticação multifator; partilhas externas protegidas por passwords e limitadas no tempo; proteção contra ataques de força bruta; auditorias de segurança regulares, internas e externas; testes

33 https://nextcloud.com/secure

de penetração regulares; cópias de segurança encriptadas onsite e offsite; atualizações automáticas do sistema e do software instalado;

- *Deteção*: análise dos ficheiros de registo do sistema; motorização dos recursos do sistema; motorização das atividades dos utilizadores; monitorização de tentativas de autenticação; deteção e ataque de forma bruta; deteção de intrusões; deteção de rootkits; deteção de ataques de força bruta e de negação de serviço; análise de padrões de atividade;
- *Resposta*: backups e snapshots ou imagens virtuais integrais para recuperação e reposição do sistema; backups da configuração do sistema; verificação regular das cópias de segurança; documentação sobre a instalação e configuração do sistema; sistemas automáticos de reconstituição do servidor (via ansible[34]); servidor secundário redundante;

A Figura 3.2, abaixo, mostra o resumo dos resultados[35] de uma auditoria de segurança efetuada regularmente ao servidor.

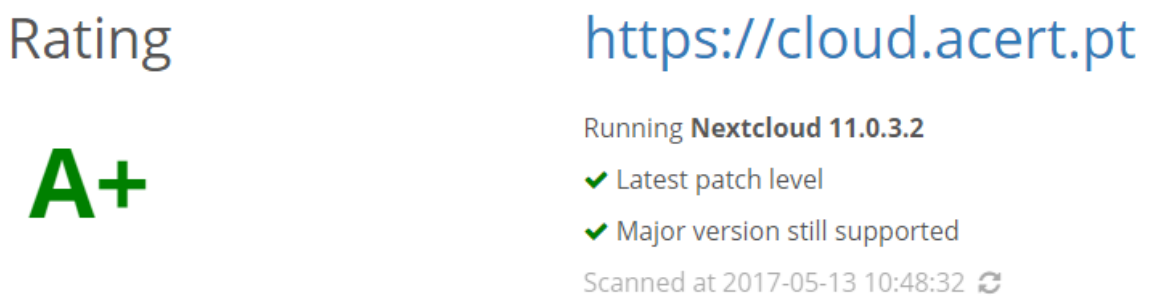


Figura 3.2: Resultados de uma auditoria externa de segurança
Fonte: https://scan.nextcloud.com/results/66b5388e-f71c-4ee9-8f19-1897e1a95ac2

Uma vez instalada e configurada a aplicação, foram criados os utilizadores e, em seguida, afetados aos grupos correspondentes à unidade ou unidades orgânicas onde desempenham as suas tarefas, segundo o anteriormente definido na Tabela 3.1, acima. Em seguida foi criada toda a estrutura hierárquica das pastas referentes ao esquema de classificação adotado e descrito em 3.4.2 Organização e estrutura das pastas, acima.

As vantagens desta solução foram sintetizadas de forma elucidativa, quando o colaborador que anteriormente relatava as suas dificuldades na gestão de reservas, partilhou a solução que ele próprio concebeu: “Agora, quando receber um pedido de reserva, posso aceder, a

34 https://www.ansible.com
35 Os resultados completos podem ser consultados no endereço https://scan.nextcloud.com/results/66b5388e-f71c-4ee9-8f19-1897e1a95ac2

partir do meu smartphone e via internet, ao ficheiro de reservas, confirmar a disponibilidade em tempo real e efetuar a marcação sem risco de overbooking".

3.4.5. Sensibilização e formação dos utilizadores

Durante as entrevistas conduzidas aos colaboradores, ficaram claras as necessidades de formação e sensibilização em diversas áreas, desde a gestão da informação até à utilização segura da internet. De forma a colmatar essas necessidades foi elaborado um plano de sensibilização e formação, em colaboração com a direção da associação, cobrindo as seguintes áreas:

- Gestão da informação;
- Segurança da informação;
- Utilização segura da internet;
- Utilização da plataforma de gestão da informação;

Uma das ações de sensibilização e consciencialização que teve mais impacto junto dos utilizadores foi a demonstração e discussão dos perigos e riscos da utilização da internet e suas consequências para a organização e para os indivíduos. No final, muitos dos participantes reconheciam desconhecer os riscos e as consequências do uso menos consciente da internet, bem como as regras e boas práticas básicas para a sua utilização, de forma de defensiva e segura. Em consequência, foram organizados diversos eventos de sensibilização e formação sobre a importância da informação e da sua segurança, bem como as formas de utilização segura da internet, nomeadamente:

- Apresentação e workshop para a consciencialização do valor da informação e a sua importância para a organização e para os indivíduos;
- Apresentação e workshop sobre a importância da segurança da informação e consequências de eventuais quebras de segurança;
- Apresentação e workshop sobre a utilização segura da internet, identificação de riscos e boas práticas para os evitar;

Na área da gestão da informação foram criados diversos documentos contemplando um conjunto de regras e boas práticas para a organização, gestão e segurança da informação.

- "*Organização da informação para quê?*": documento de sensibilização sobre o valor da informação para a organização e a importância da sua gestão e organização;

- "*Boas práticas para a nomeação de ficheiros*": documento de sensibilização sobre a importância dos nomes de pastas e ficheiros e conjunto de regras e boas práticas para a sua seleção;
- "*Hierarquia das pastas e ficheiros*": conjunto de regras e boas práticas a observar na utilização da hierarquia de pastas e ficheiros no sistema de gestão da informação;
- "Regras de proteção e distribuição da informação": conjunto de regras para a classificação do grau de confidencialidade da informação;

Estes documentos foram ou serão oportunamente apresentados aos colaboradores, em diversas ações de formação em contexto de trabalho real, demonstrando a sua aplicação e integração prática nos processos de trabalho quotidianos. Com o objetivo de estarem sempre acessíveis a partir de diferentes dispositivos, os documentos foram também disponibilizadas versões em formato de texto, HTML e PDF, na pasta de raiz de cada utilizador e de cada grupo do sistema de gestão da informação.

Por fim, foram também realizadas ou estão ainda em curso diversas ações de formação e tutoria sobre a utilização do sistema de gestão da informação:

- Utilização do sistema de gestão da informação e a aplicação prática das regras de organização e gestão da informação;
- Integração das diversas funcionalidades nos processos de trabalho;
- Integração e utilização das diversas aplicações e em diferentes dispositivos;
- Boas práticas de trabalho colaborativo;

3.5. Resultados obtidos e objetivos futuros

Dado que a implementação do sistema de gestão da informação é um processo atualmente em curso de realização e cuja conclusão está prevista para dezembro de 2017 não é possível apresentar conclusões definitivas. O projeto prevê três fases principais, sendo a primeira de preparação e demonstração de uma prova de conceito funcional, a segunda de arranque, limitado a um grupo piloto restrito e, posteriormente, o alargamento a toda a organização.

À data atual está concluída a fase de preparação, englobando:

- Levantamento e análise das necessidades de organização e gestão da informação;
- Desenvolvimento do modelo de gestão da informação;

- Instalação e configuração da plataforma informática;
- Criação dos diferentes manuais de regras e boas práticas;

Em curso de realização, sob a forma de projeto piloto envolvendo apenas as unidades organizacionais “Direção” e “Comunicação”, encontram-se as seguintes etapas:

- Sensibilização e formação dos utilizadores;
- Instalação e configuração dos equipamentos;
- Implementação do modelo de gestão da informação;
- Migração da informação para a nova plataforma;

Esta segunda fase piloto, com data de conclusão prevista para julho de 2017, irá permitir testar o modelo e a plataforma, recolher e analisar a experiência e retorno dos utilizadores e, eventualmente, introduzir correções e ajustes que se verifiquem necessárias.

Na terceira e última fase, com início previsto para setembro de 2017 e que se desenrolará até dezembro de 2017, as etapas desenvolvidas com o grupo piloto serão progressivamente alargadas a toda a organização.

Em análise está também a possibilidade de uniformização das principais aplicações utilizadas pela organização. Atualmente, são utilizadas, em simultâneo, diversas aplicações e versões de clientes de correio eletrónico, processamento de texto, folhas de cálculo, agenda e contactos, o que gera frequentemente diversos problemas de compatibilidade e portabilidade da informação. A uniformização das aplicações, privilegiando a utilização de standards abertos, versões de utilização livre e disponíveis em diferentes plataformas, permitiria uma melhor gestão da informação, facilidade de utilização, melhor colaboração e integração com a plataforma de gestão da informação ou com outros sistemas, como, por exemplo, o site web da organização.

4. Conclusão

Neste estudo de caso procurou-se compreender de que forma uma associação cultural está a conduzir a adoção de um sistema de gestão da informação baseado na cloud, capaz de responder, em segurança, às necessidades impostas pelas exigências do trabalho colaborativo, pela utilização e diversificação de novos dispositivos, como os smartphones e tablets, e pela grande mobilidade dos seus colaboradores.

Durante a fase inicial deste estudo verificou-se que, embora a informação fosse considerada importante pelos utilizadores, a perspetiva vigente era a de armazenamento da informação, resultante de uma necessidade pessoal e não com o intuito de a gerir, valorizar e colocar ao serviço da organização, alinhada com o seu modelo de negócio. Por seu lado, também o trabalho colaborativo e a partilha de informação eram geridos de acordo com as necessidades e competências informáticas individuais e não de forma normalizada e organizada. De forma semelhante, não existia uma verdadeira política de segurança da informação nem a consciencialização da sua importância, ou ainda as eventuais consequências de uma utilização menos acautelada da internet. Como consequência, foram consideradas de grande importância e impacto para os utilizadores as ações de sensibilização e formação iniciais em áreas como a importância, valorização e gestão da informação, bem como a tomada de consciência dos riscos, consequências e boas práticas na utilização quotidiana da internet.

Esta nova consciencialização para a importância, valor estratégico e necessidade de gestão eficaz da informação abriu as portas para um trabalho de fundo de organização informação, envolvendo a direção e os colaboradores, que com a consciência das limitações existentes e necessidades constatadas, foram capazes de desenvolver um conjunto de especificações e requisitos para o seu sistema de gestão de informação, bem como um plano de ação para a sua implementação e adoção.

Neste âmbito foi elaborado um plano de gestão e classificação da informação, envolvendo, no seu desenvolvimento, a direção e os colaboradores da organização. Desta forma, conseguiu-se, para além de um plano de gestão da informação alinhado com as necessidades da organização, uma melhor aceitação e compreensão daquele pelos colaboradores, o que facilitou a sua adoção e integração nas tarefas quotidianas da organização.

Paralelamente, foi criada e configurada a plataforma informática de suporte ao plano de gestão da informação, onde foram inscritos os utilizadores e grupos funcionais e onde foi

criada a estrutura de pastas previstas pelo plano de classificação da informação. Esta plataforma, complementada com ferramentas de pesquisa avançada, partilha de informação e trabalho colaborativo, passou a ser o ponto de acesso centralizado e uniformizado para a gestão de toda a informação produzida ou adquirida pela organização.

Especial cuidado foi colocado na segurança da informação, de forma garantir a sua disponibilidade, confidencialidade e integridade, onde se procuraram implementar as melhores práticas, não só do ponto de vista técnico e tecnológico, mas também tendo em conta a componente humana, ao integrar um conjunto de boas práticas e regras básicas de segurança na execução das tarefas quotidianas dos utilizadores.

Um fator decisivo para o sucesso da adoção do sistema de gestão da informação foi o reconhecimento da importância do papel que o fator humano desempenha na gestão e segurança da informação. Tendo em conta esta visão, procurou-se envolver, desde o início do processo, os utilizadores, tendo estes sido convidados a partilhar as suas dificuldades e necessidades e a dar também o seu contributo na busca de soluções e na definição das especificações do sistema de classificação da informação. Em complemento, a implementação deste plano de gestão da informação foi suportada por diversas ações de tutoria, formação e sensibilização dos utilizadores e apoiada em documentação de suporte, contendo um conjunto de procedimentos, regras e boas práticas de utilização quotidiana.

Sendo este um projeto em curso e numa fase inicial, os dados que dispomos até ao momento não nos permitem tecer conclusões de forma sustentada e definitiva. Assim, ainda que qualquer conclusão seja prematura, os indicadores que dispomos, baseados nos resultados até agora alcançados, permitem-nos identificar algumas tendências relativamente ao impacto e às mudanças que a adoção do sistema de gestão da informação está a operar, quer a nível da organização, quer a nível individual.

Assim, a primeira e mais importante tendência observável é o gradual abandono da necessidade de arquivo da informação para simples cumprimento de obrigações legais ou históricas e a adoção da visão da informação como um ativo da organização, com valor estratégico, capaz de sustentar o seu modelo de negócio e oferecer vantagens competitivas.

Como consequência, a organização e gestão da informação foi entendida e interiorizada pelos colaboradores não apenas como uma necessidade, mas também como uma vantagem, capaz de acrescentar valor à informação, facilitar as tarefas de pesquisa e recuperação de informação e melhor o desempenho individual e coletivo. Paralelamente, o nível de

exigência, no que diz respeita às necessidades de organização e gestão da informação aumentou substancialmente, o que se traduziu na elaboração de uma extensa e detalhada lista de requisitos que o sistema de gestão da informação deveria cumprir para satisfazer as necessidades da organização.

Também problemas e preocupações concretas com que a organização se debatia de forma quotidiana, como as dificuldades de partilha ou acesso atempado à informação, o trabalho colaborativo, a duplicação de informação, a pesquisa centralizada de diferentes tipologias de informação ou o acesso a partir dos dispositivos pessoais, como os tablets ou smartphones, estão a obter uma solução concreta e satisfatória com a implementação da nova solução.

A criação de condições e adição de ferramentas de suporte à colaboração, como a criação de equipas virtuais, a edição conjunta de documentos ou as possibilidades oferecidas pelas videoconferências, está a ser antecipada com grandes expetativas, dada a importância com que o trabalho colaborativo se reveste para a organização.

Não menos importante, a adoção do sistema de gestão da informação está já a ter um impacto real que se traduz numa melhoria dos resultados da organização e do seu modelo de negócio e no desempenho individual dos seus colaboradores, o que podemos constatar em exemplos concretos como a eliminação do risco de overbooking acidental na reserva de bilhetes ou a facilidade de partilha da informação com entidades e parceiros externos.

Por fim, pudemos constatar um resultado não totalmente previsto, mas avaliado de forma muito positiva pela organização e pelos seus colaboradores, que foi a tomada de consciência para uma melhor utilização da internet, resultante das ações de formação e sensibilização iniciais, em que os utilizadores sentiram ter adquirido competências que lhes permitem conhecer, compreender e avaliar melhor os riscos e perigos e adotar um conjunto de hábitos e boas práticas para uma utilização segura da internet.

Como trabalho futuro, será interessante verificar de que forma a implementação de um sistema de gestão da informação transformou a organização, a sua forma de trabalhar e o seu modelo de negócio. Também a adoção gradual de uma consciência orientada para a gestão da informação como ativo estratégico e de grande valor está apenas agora a ser assimilada pelos colaboradores, o que deixa espaço para investigar de que forma essa consciencialização vai transformar os seus hábitos de trabalho e qual o seu impacto na produtividade individual e coletiva.

Bibliografia

Abelson, H. (1999). *Architects of the Information Society: Thirty-Five Years of the Laboratory for Computer Science at MIT*. Cambridge, MA: MIT Press

Adachi, T. (2004). *Gestão de Segurança em Internet Banking*. Dissertação de Mestrado. Fundação Getúlio Vargas - Administração. São Paulo.

Alarcão, I. (2003). *Professores reflexivos em uma escola reflexiva*. São Paulo: Cortez Editora.

Alves, M. (Jornalista), Silva, J. (Imagem), Carvalho, R.G. (Direção), & Vieira, A. (Direção). 2015. Impossível é só um exagero para difícil [Reportagem televisiva]. *Reportagem Especial*. Lisboa: SIC Notícias.

Amaral, L. (1994). *PRAXIS: um referencial para o planeamento de sistemas de informação*. Obtido de http://repositorium.sdum.uminho.pt/handle/1822/49

Araújo, E.E.de. (2005). *A vulnerabilidade humana na segurança da informação*. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) – Faculdades Uniminas, Uberlândia.

Ashby, W.R. (1956). *An Introduction to Cybernetics*. London: Chapman and Hall, Ltd.

Beal, A. (2005). *Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. São Paulo: Atlas.

Boavida, A., & Ponte, J.P.da. (2002). Investigação colaborativa: Potencialidades e problemas. *Reflectir e investigar sobre a prática profissional*, (1), 43–55.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, *25*(6), 599–616.

Camp, L.J. (2001). *Trust and risk in Internet commerce*. Cambridge, MA.: MIT Press.

Charbonneau, N., & Robert, M. (Eds.). (2001). *La gestion des archives photographiques*. Sainte-Foy: Presses de l'Université du Québec.

Choo, C.W. (2003). *Gestão de informação para a organização inteligente: a arte de explorar o meio ambiente*. Porto: Caminho.

Choo, C.W. (2006). *A organização do conhecimento: como as organizações usam para criar significado, construir conhecimento e tomar decisões.* São Paulo: Editora Senac.

Choo, C.W., Bergeron, P., Detlor, B., & Heaton, L. (2008). Information culture and information use: An exploratory study of three organizations. *Journal of the American Society for Information Science and Technology*, *59*(5), 792–804. https://doi.org/10.1002/asi.20797

Collet, A. (2012). Le plan de classement des documents dans un environnement électronique: concepts et repères. *La Gazette des archives*, *228*(4), 245–264.

Couture, C. (Ed.). (1999). *Les fonctions de l'archivistique contemporaine*. Sainte-Foy: Presses de l'Université du Québec.

Davenport, T.H. (2000). *Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação*. São Paulo: Futura.

Davenport, T.H., & Prusak, L. (1998). *Conhecimento empresarial: como as organizações gerenciam o seu capital intelectual*. Rio de Janeiro: Campus.

Detlor, B. (2010). Information management. *International Journal of Information Management*, *30*(2), 103–108. https://doi.org/10.1016/j.ijinfomgt.2009.12.001

Drucker, P.F. (1998). The Coming of the New Organization. *Harvard Business Review on Knowledge Management*, 1–19. Harvard Business School Press.

Fortin, M.F. (2009). *Fundamentos e Etapas no Processo de Investigação*. Loures: Lusodidacta.

Frunzeanu, M. (2015). Using Wikis, Word Clouds and Web Collaboration in Romanian Primary Schools. *Procedia - Social and Behavioral Sciences*, *180*, 580–585. https://doi.org/10.1016/j.sbspro.2015.02.163

Gray, B. (1989). *Collaborating: finding common ground for multiparty problems* (1st ed). San Francisco: Jossey-Bass.

Hashizume, K., Rosado, D.G., Fernández-Medina, E., & Fernandez, E.B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 5.

ISO 15489-1 (2001). *Information and documentation — Records management — Part 1: General*. International Organization for Standardization. Geneva, Switzerland.

ISO 15489-1 (2016). *Information and documentation — Records management — Part 1: Concepts and principles*. International Organization for Standardization. Geneva, Switzerland.

ISO/IEC 27001 (2013). *Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization, International Electrotechnical Commission. Geneva, Switzerland.

ISO/IEC 27002 (2013). *Information technology — Security techniques — Code of practice for information security controls*. International Organization for Standardization, International Electrotechnical Commission. Geneva, Switzerland.

Keakopa, S., Millar, L., O'Shea, G., Nordland, L. P., Suderman, J., Ardern, C., … others. (2009). Understanding the Context of Electronic Records Management. *Training in Electronic Records Management.* International Records Management Trust. London.

Kleinrock, L. (1996). Nomadicity: anytime, anywhere in a disconnected world. *Mobile Networks and Applications*, *1*(4), 351–357.

Kleinrock, L. (2001). Breaking loose. *Communications of the ACM*, *44*(9), 41–46.

Kleinrock, L. (2003). An Internet vision: the invisible global infrastructure. *Ad Hoc Networks*, *1*(1), 3–11. https://doi.org/10.1016/S1570-8705(03)00012-X

Krippendorff, K. (1973). *Some principles of information storage and retrieval in society*. Retrieved from http://eric.ed.gov/?id=ED084001

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., … Wolf, S. (1999). A brief history of the Internet. *arXiv preprint cs/9901011*. Obtido de https://arxiv.org/abs/cs/9901011

Lima, J.A. (2002). *As culturas colaborativas nas escolas. Estruturas, processos e conteúdos*. Colecção Currículo, Políticas e Práticas 15. Porto: Porto Editora.

MacMullin, S.E., & Taylor, R.S. (1984). Problem dimensions and information traits. *The Information Society*, *3*(1), 91–111.

Mas, S. (2007). *Schémas de classification et repérage des documents administratifs électroniques dans un contexte de gestion décentralisée des ressources informationnelles*. Thèse de doctorat. École de bibliothéconomie et des sciences de l'information, Faculté des arts et des sciences, Université de Montréal.

Mell, P., Grance, T., & others. (2011). *The NIST definition of cloud computing*. Obtido de http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

Netto, A.S., & Silveira, M.A.P. (2007). Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. *JISTEM-Journal of Information Systems and Technology Management*, *4*(3), 375–397.

O'Brien, J.A., & Marakas, G.M. (2007). *Enterprise information systems* (13th ed., internat. ed). Boston, Mass: McGraw-Hill.

O'Reilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & strategies*, (1), 17.

Oliva, J.L. (2016). *ACERT XL – O fio, a trama e a urdideira*. Porto: Edições Afrontamento.

Parkes, L.L.W. (Producer), & Robinson, P.A. (Director). (1992). *Sneakers* [Filme]. Estados Unidos da América: Universal Studios.

Peixoto, M.C.P. (2006). *Engenharia social e segurança da informação na gestão corporativa*. Rio de Janeiro: Brasport.

Reis, C. (1993). *Planeamento estratégico de sistemas de informação*. Lisboa: Editorial Presença.

Ribeiro, F. (2016). *Servidor Debian 8 'Jessie'*. Obtido 29 de Março de 2017, de https://servidordebian.org/pt/start

Ribeiro, J.M.S., (2007). Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. *Cadernos UniFOA*, 5, 11-21.

Schmidt, E. (2006). Search Engine Strategies Conference. Obtido 23 de Fevereiro de 2017, de https://www.google.com/press/podium/ses2006.html

Sêmola, M. (2003). *Gestão da segurança da informação*. Obtido de http://www.sciencedirect.com/science/book/9788535211917

Souza, H.J., (1992).*As ONGs na década de 90. Desenvolvimento, cooperação internacional e as ONGs*. Rio de Janeiro: IBASE/PNUD.

Stair, R.M., & Reynolds, G.W. (2012). *Fundamentals of information systems*. Boston: Course Technology/Cengage Learning.

Stewart, H. (1997). Metaphors of interrelatedness: Principles of collaboration. In H. Christiansen, L. Goulet, C. Krentz & M. Maeers (Eds.), *Recreating relationships: Col-laboration and educational reform* (pp. 27-53). New York: State University of New York.

Su, C.-J., & Chiang, C.-Y. (2012). Enabling successful Collaboration 2.0: A REST-based Web Service and Web 2.0 technology oriented information platform for collaborative product development. *Computers in Industry*, *63*(9), 948–959. https://doi.org/10.1016/j.compind.2012.08.018

Taylor, R.S. (1986). *Value-added processes in information systems*. Norwood, N.J: Ablex Pub. Corp.

Terra, J.C.C., & Gordon, C. (2002). *Portais corporativos: a revolução na gestão do conhecimento*. São Paulo: Negócio Editora.

Tractenberg, L., & Struchiner, M. (2010). A emergência da colaboração na educação e as transformações na sociedade pós-industrial: em busca de uma compreensão problematizadora. *Boletim Técnico do SENAC*, *36*(2), 65–77.

Trigo Limpo Teatro ACERT (2001). *Trigo Limpo Teatro ACERT: 25 anos a fabricar sonhos*. Tondela: ACERT.

Vaquero, L.M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, *39*(1), 50–55.

Wilson, T. (1989). Towards an information management curriculum. *Journal of Information Science*, *15*(4–5), 203–209.

Wilson, T.D. (2003). Information management. In Feather, J., & Sturges, R. P. (2003). *International encyclopedia of information and library science*. London; New York.

Winkler, J. R. (2011). *Securing the cloud: cloud computer security techniques and tactics*. Waltham, MA: Syngress/Elsevier.

Apêndices

Apêndice 1: Organização da informação para quê?

Organização de ficheiros para quê?

> Quantas vezes já procurou um documento, que se lembra de ter visto ou consultado, não sabe bem onde nem quando? E quantas vezes esse documento continha informação essencial para preparar a reunião com aquele cliente tão importante? É azar? Não, é apenas má gestão da informação!

A informação produzida ou adquirida por uma empresa ou instituição representa um dos seus mais valiosos recursos. Ela contém todo historial da empresa, acumula todo o seu *know-how*, constitui uma base de trabalho inestimável e representa, na prática, o seu ADN.

A informação constitui também, e ao mesmo tempo, um registo e uma prova das ações levadas a cabo pela empresa ou instituição. Atesta a conformidade e é requerida para o cumprimento de diversos requisitos legais, tais como as obrigações fiscais, os contratos celebrados ou normas de qualidade e segurança.

Por consequência, uma boa gestão da informação, sustentada por uma cuidadosa organização das pastas e dos ficheiros, é simplesmente uma boa prática. Aumenta a eficiência e produtividade individual e coletiva, uniformiza métodos de trabalho e procedimentos, promove a segurança da documentação, centraliza e impede a duplicação e degradação da informação, facilita a sua criação, manutenção e partilha e mantém a organização em linha com a sua visão, missão e objetivos.

Benefícios de uma boa organização de ficheiros

Os benefícios de uma boa organização de ficheiros são imensos. A título de exemplo, poderemos salientar apenas alguns:

- Organiza a informação de uma maneira lógica, coerente, consistente e familiar;
- Facilita a criação, manutenção e partilha de informação;
- Permite localizar rapidamente os documentos de um departamento, de um projeto ou de um cliente;
- Mantém o histórico das atualizações de cada ficheiro;
- Contribui para a segurança da informação;

- Facilita a definição e o cumprimento das regras e permissões de acesso, edição e partilha;
- Facilita a segurança e a reposição de documentos em caso de catástrofe;
- Evita duplicação de documentos, com conteúdos diferentes;
- Facilita o trabalho colaborativo;
- Aumenta a eficiência e a produtividade;
- Facilita a integração e formação de novos colaboradores;
- Mantém uma imagem gráfica coerente da organização;
- Uniformiza documentos e procedimentos;
- Facilita a criação, leitura e interpretação de documentos e formulários;

Apêndice 2: Boas práticas para a nomeação de ficheiros

Boas práticas para a seleção de nomes de ficheiros

A utilização de alguns critérios básicas na escolha dos nomes de pastas e ficheiros é fundamental para uma boa organização documental, e pode proporcionar uma enorme diferença na facilidade de pesquisa de documentos e na antevisão do seu assunto ou conteúdo. A título de exemplo, listamos algumas boas práticas para a correta nomeação de ficheiros e pastas.

Uso de dígitos

Usar dígitos no início do nome para ordenar documentos ou pastas numa sequência lógica.

- Ex: `01Recebidos`, `02Enviados`, `03Rascunhos`.

Usar dígitos no final do nome para distinguir diversos ficheiros relacionados ou do mesmo tipo.

- Ex: `foto001.jpg`, `foto002.jpg`, etc.

Usar dígitos em função da quantidade de documentos a nomear.

- Ex: `01` para menos de 100 documentos ou `001` para até 999 documentos.

Não usar numeração romana, exceto se esta for parte integrante do nome.

- Ex: Usar `MacOSX` ou `XIICongressoNacional`.
- Ex: Usar `Foto014.jpg` em vez de `FotoXIV`.jpg.

Uso de caracteres

Não usar caracteres reservados pelo sistema operativo.

- Ex: Não usar os seguintes caracteres reservados: `~`, `!`, `@`, `#`, `$`, `%`, `^`, `&`, `*`, `(`, `)`, `` ` ``, `;`, `<`, `>`, `?`, `[`, `]`, `{`, `}`, `'`, `"`, `|` ou `.`.

Não usar caracteres especiais que apenas estão disponíveis num idioma ou tipo de teclado.

- Ex: Usar `Coordenacao` em vez de `Coordenação`.
- Ex: Usar `EyupDoganMiszrakci.doc` em vez de `EyüpDoğanMızrakçı.doc`.

Em nomes compostos, usar a primeira letra de cada palavra em maiúsculas e as restantes em minúsculas (formato vulgarmente conhecido como *CamelCase*).

- Ex: `PequenoGrandePolegar`.

Respeitar o limite de caracteres imposto pelos sistemas operativos.

- Ex: A família de sistemas operativos *Microsoft Windows* e *Mac OS X* têm um limite de 255 caracteres para o caminho completo dos ficheiros.

Não usar espaços.

- Ex: Usar `FichaTecnica.doc` em vez de `Ficha Tecnica.doc`.

Uso de termos

Evitar o uso de preposições (`de`, `do`, `em`, `a`, `para`, `sem`, `com`, etc).

- Ex: Usar `RelatorioAtividades.xls` em vez de `RelatorioDeAtividades.xls`.

Evitar repetições e redundâncias nos nomes de pastas e ficheiros.

- Ex: Usar `/Festivais/Teatro/Finta/2017/Fotos/Casa01.jpg` em vez de `/Festivais/Teatro/Finta/2017/FotosFinta2017/Fotos/Casa01.jpg`.

Tipologias documentais

Definir nomes standard para definir o tipo de documento.

- Ex: `Memorando`, `Relatorio`, `Convite`, `Ata`, etc.

Evitar incluir o tipo de documento no nome (que pode ser facilmente inferido a partir da extensão).

- Ex: Usar `Masala01.jpg` em vez de `FotosMasala001.jpg`.
- Ex: Evitar nomes como `Documento de texto.doc` ou `Folha de Cálculo.xls`.

Nomes de pessoas

Usar primeiro o apelido seguido das iniciais do nome próprio ou o primeiro nome por extenso, para distinguir nome idênticos.

- Ex: `RibeiroF` ou `RibeiroFernando` para distinguir de `RibeiroFrancisco`.

Evitar usar os títulos académicos ou de cortesia, exceto quando absolutamente necessário.

- Ex: Usar `RibeiroFernando` em vez de `SrRibeiroFernando` ou `RibeiroSrFernando`.

Datas

Os nomes de ficheiros ou pastas referentes a eventos recorrentes devem incluir a data no formato apropriado para a periodicidade.

- Ex: `Orcamento2015.doc` ou `Vendas2015-10-29.xls`.

Usar o standard *ISO 8601*, indicando o ano, o mês e o dia separados com um hífen no formato: `AAAA-MM-DD`.

- Ex: `2015-10-29`.

Não usar a barra (`/`) como separador nas datas, dado ser um carater especial reservado em diversos sistemas operativos.

- Ex: Usar `2015-10-29` em vez de `2015/10/29`.

Usar o formato `AAAA-WSS-D` para indicar a semana e o dia.

- Ex: `2015-W44-4`.

Usar sempre quatro dígitos para indicar o ano afim de evitar ambiguidades.

- Ex: Não usar `12-11-10` (a data refere-se a 2012, a 2010 ou a qualquer outro século?).
- Ex: Usar `2012-11-10`.

Versões do mesmo ficheiro

Incluir sempre informações sobre a versão em documentos que são alterados ou revistos com frequência.

- Ex: `GuiaoV06.doc`.

Indicar o número da versão ou revisão no final do nome do documento.

- Ex: Usar `GuiaoV06.doc` em vez de `V06Guiao.doc`.

Incluir o estado de desenvolvimento do documento, em conjunto com a versão (rascunho, revisão, final, etc.):

- Ex: `GuiaoSilkaDraft01.doc` ou `GuiaoSilkaV01.doc`.

Outros critérios relevantes

Usar nomes curtos mas representativos do assunto do documento.

- Ex: Usar `ReceitaBilheteira.xls` em vez de `RelacaoDosBilhetesVendidos.xls`.

Usar os termos mais relevantes no início do nome do documento.

- Ex: Usar `GuiaoSilkaV6.doc` em vez de `V6SilkaGuiao.doc`.

Usar pastas e subpastas para auxiliar a organização dos ficheiros e manter os nomes curtos.

- Ex: `/Festivais/Teatro/Finta/2017/Istambul001.jpg`.

Na criação de pastas e subpastas, começar pelos elementos mais genéricos e continuar com os elementos cada vez mais específicos.

- Ex: `/Parceiros/Portugal/Porto/IPP/Protocolos/`.

Incluir em cada pasta um documento com as regras de nomeação de ficheiros:

- Ex: incluir um documento `LEIAME.TXT` ou `LEIAME.PDF` com as regras de nomeação de ficheiros a guardar nessa pasta.

Ter em conta as limitações impostas pelo sistema ou pelas tecnologias utilizadas em todo o processo de gestão da documentação.

- Ex: Certos leitores de códigos de barras tem um número reduzido de caracteres que podem reconhecer e gerir: o conjunto de caracteres *Code 39* para leitores de códigos de barras suporta apenas 43 caracteres: as letras `A` a `Z`, os algarismos `0` a `9`, e os carateres especiais `-`, `.`, `$`, `/`, `+`, `%` e ` `(espaço).

Todos os documentos gerados em formato *PDF* deverão respeitar a norma *ISO 19005-1 PDF/A-1* para garantir a sua preservação a longo prazo.

Apêndice 3: Hierarquia das pastas e ficheiros

Organização de pastas para quê?

Se pensarmos que uma organização está dividia em departamentos, estes em secções, e subsecções e cada uma fornece ainda diversos produtos ou serviços, torna-se clara a necessidade de separar e organizar os diferentes tipos de informação de cada unidade organizacional. Uma estrutura de pastas permite fazer essa organização da informação de acordo com o modelo de negócio da organização.

Uma estrutura de pastas facilita oferece diversas vantagens, das quais listamos algumas, a título de exemplo:

- Organiza a informação de forma lógica, coerente e de acordo com as regras de negócio;
- Facilita a criação, pesquisa e recuperação da informação;
- Facilita o trabalho colaborativo e a partilha de ficheiros;
- Facilita a gestão das regras e permissões de acesso, edição e partilha;
- Facilita a proteção e distribuição da informação;
- Reforça a segurança da informação.

Com base nestas premissas, foi definido um conjunto de regras e boas práticas a observar para uma correta utilização e gestão da hierarquia de pastas.

Boas práticas na utilização de hierarquia de pastas

- Os nomes das pastas e ficheiros deverão respeitar as regras de nomeação de pastas e ficheiros definidos no manual de boas práticas para a nomeação de ficheiros.
- Os nomes das pastas deverão ser claros, coerentes, relevantes e ilustrativos das categorias que representam.
- Sempre que possível, os nomes das pastas deverão ser normalizados e transversais às diversas unidades funcionais, de forma a facilitar a organização, pesquisa e recuperação da informação.
- A profundidade da hierarquia deve ser apenas a mínima necessária, evitando a criação de um excessivo número de subpastas, por forma a facilitar a legibilidade, navegação, pesquisa e recuperação da informação.

Regras de utilização da hierarquia de pastas

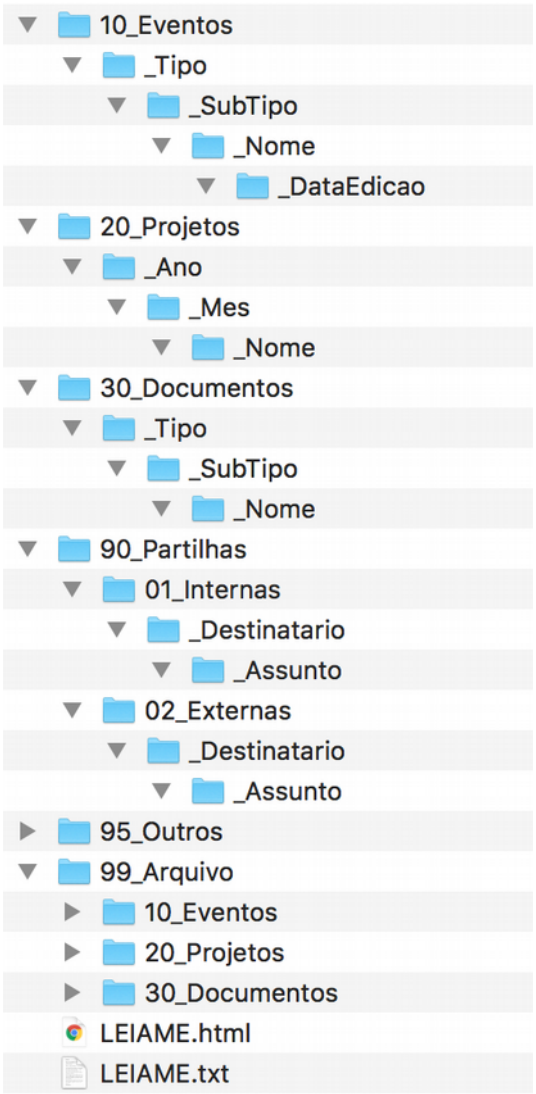
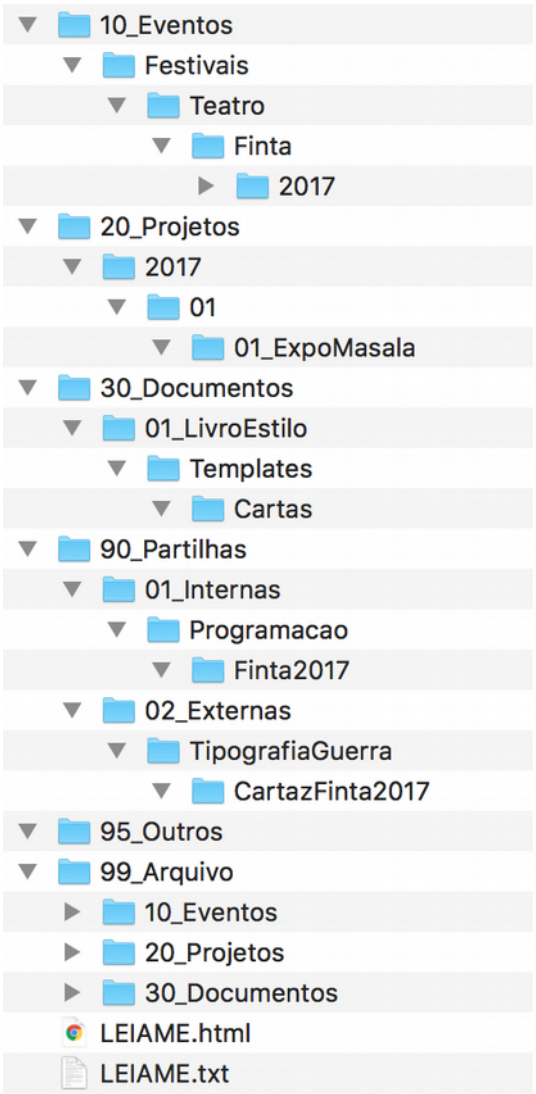
4. Cada unidade funcional dispõe de uma pasta no topo da hierarquia do repositório, identificada pelo nome curto da unidade funcional. Esta pasta será partilhada, com direitos de leitura e escrita, por todos os membros dessa unidade funcional. No primeiro nível foram criadas as pastas “`Acert`”, “`Basquetebol`”, “`Comunicação`”, “`Coordenacao`”, “`Direcao`”, “`Escalada`”, “`Programacao`”, “`Secretariado`”, “`ServicoEducativo`”, “`ServicoTecnico`” e “`TrigoLimpo`”.
5. Num segundo nível, deverão existir, obrigatoriamente, as seguintes pastas:
   a. `10_Eventos`: Informação relativa a eventos recorrentes;
   b. `20_Projetos`: Informação relativa a projetos e eventos não recorrentes;
   c. `30_Documentos`: Informação utilizada regulamente pelos serviços permanentes e necessária para o desempenho das tarefas quotidianas do serviço;
   d. `90_Partilhas`: Informação partilhada dentro da organização (entre grupos) ou fora da organização (com parceiros externos);
   e. `95_Outros`: Informação não classificável nas categorias existentes. O conteúdo desta pasta poderá indicar a necessidade de criação de novas categorias ou subcategorias que permitam a correta classificação desta informação.
   f. `99_Arquivo`: Informação em fase não ativa ou que deva respeitar um período de arquivo antes da sua destruição, de acordo com a política de retenção. A estrutura deverá reproduzir, a partir desta pasta, a hierarquia de segundo nível. (Ex: `99_Arquivo/10_Eventos/.../`).

   Em função das necessidades específicas de cada unidade funcional poderão ser criadas outras pastas, que deverão respeitar a nomenclatura indicada.
6. No terceiro nível e seguintes deverão ser criadas pastas e subpastas da forma que melhor ilustre cada um dos processos ou objetivos a realizar dentro da categoria representada pelo segundo nível.
   a. `10_Eventos`: Pasta e subpastas com o tipo e subtipo de evento, nome e periodicidade de ocorrência. Exemplo:
      - `10_Eventos/Festivais/Teatro/Finta/2016/`
      - `10_Eventos/Ingles/Iniciacao/2016-17/`
      - `10_Eventos/Competicoes/Nacionais/2016-17/`

b. `20_Projetos`: Pasta e subpastas com a data e nome do projeto. Exemplo:
    - `20_Projetos/2017/01/AgendaACERT/`
    - `20_Projetos/2017/03/ExpoMASALA/`
c. `30_Documentos`: Pasta e subpastas representativas da tipologia documental. Poderão ser complementadas com outros elementos identificativos relevantes. Exemplo:
    - `30_Documentos/01_Modelos/Cartas/`
    - `30_Documentos/02_Correspondencia/01_Recebida/2017/01/`
    - `30_Documentos/02_Correspondencia/02_Enviada/2017/01/`
d. `90_Partilhas`: Pastas e subpastas representativas do tipo de partilha (interna ou externa), destinatário e assunto. Estas partilhas devem ter sempre um caráter temporário e limitado no tempo. Exemplo:
    - `90_Partilhas/01_Internas/Comunicacao/CartazFinta2017/`
    - `90_Partilhas/02_Externas/TipografiaGuerra/CartazFinta2017/`

Utilização da hierarquias de pastas

A tabela abaixo exemplifica a utilização da hierarquia de pastas proposta neste documento, comparando uma unidade funcional abstrata com a utilização prática na unidade "Comunicação".

Unidade funcional abstrata	Unidade funcional "Comunicação"
	

Apêndice 4: Regras de proteção e distribuição da informação

Proteção da informação para quê?

Todos os dias, produzimos e partilhamos informações que são necessárias, ou mesmo críticas para o bom funcionamento da organização, a fim de aumentar os negócios, construir e manter a confiança e credibilidade junto dos nossos associados, clientes e parceiros de negócios.

A maioria dos países aprovou leis para proteger os direitos individuais, a propriedade intelectual, a liberdade de imprensa, etc. Estas leis diferem entre países e devemos garantir que as cumprimos. Num ambiente de grande concorrência e legislação exigente, as informações que são parte integrante do sucesso da nossa organização devem ser protegidas contra a perda, uso ou divulgação indevidas, de forma proporcional ao seu valor para a organização.

A segurança da informação é uma combinação de medidas que garantem:

- a disponibilidade de informação aos utilizadores autorizados sempre que necessário;
- a integridade da informação, ou seja, a sua exatidão;
- a confidencialidade das informações que garantem que apenas as pessoas autorizadas tenham acesso.

Como determinamos quais as informações a proteger?

As normas de classificação da informação diferenciam entre a informação sensível e que requer medidas de segurança especiais e a informação menos valiosa que não necessita de tratamento especial.

Quem é responsável pela segurança da informação?

As responsabilidades estão distribuídas da seguinte forma:

- As regras de classificação das informações implementadas pelos responsáveis para as necessidades dos seus respetivos departamentos, de acordo com as instruções definidas pela Direção da organização e sintetizadas neste documento.
- Os gestores do sistema de informação realizam o controlo e monitorização diária do Sistema de Informação da organização e asseguram a disponibilidade, integridade e confidencialidade das informações alojadas no sistema.

- Por último, é da responsabilidade de todos aplicar corretamente e as medidas de segurança.

Regras e diretrizes para a classificação da organização

A organização adotou padrões e regras de classificação para simplificar a implementação e aplicação efetivas da segurança da informação. Todas as informações utilizadas pela organização deverão ser rotuladas de acordo com um dos três níveis de classificação: *Confidencial*, *Interna* ou *Público*. Como tal, esta informação de classificação deve estar claramente indicada em todos os documentos produzidas ou adquiridas pela organização.

Classificação	Confidencial	Interna	Pública
Definição	Toda a informação cuja perda, modificação, uso indevido ou divulgação, sob qualquer forma ou meio, possa causar danos à reputação, quota de mercado ou situação económica e financeira da organização, dos seus colaboradores, associados, clientes ou parceiros de negócio.	Toda a informação utilizada, de forma quotidiana, pelos colaboradores no desempenho das suas funções e cuja divulgação possa comprometer os objetivos da organização ou afetar, os seus colaboradores, associados, clientes fornecedores, ou parceiros de negócio.	Toda a informação de livre acesso produzida ou adquirida com o objetivo de ser disponibilizada ao público em geral e destinada a ser distribuída fora da organização.
Acesso e distribuição	Restrito a colaboradores da empresa com justificada necessidade de conhecimento.	Restrito aos colaboradores da organização.	Engloba apenas as informações especificadas pela direção da organização ou direção de marketing e comunicação a serem divulgadas ao público em geral ou aos órgãos de comunicação.
Informação	• Planos e estratégias de negócio; • Políticas comerciais, negociações de contratos, lista de clientes e prospetos, propostas de negócio, registo de vendas; • Informações sobre contratos, propostas, faturas, formas de pagamento; • Informações sobre clientes e parceiros; • Propriedade intelectual; • Informações de inteligência; • Informações financeiras não incluídas nos relatórios anuais; • Informações sobre os colaboradores, a nível individual ou familiar, profissional, de saúde, bancárias, etc.; • Lista de associados, quotas e pagamento; • Dados bancários;	• Listas de contactos; • Comunicações internas; • Procedimentos e regras internas; • Manuais técnicos; • Listas de materiais; • Registos de reuniões internas; • Memorandos de trabalho, listas de preços, guias de vendas;	• Material de marketing e comunicação; • Relatórios e publicações anuais; • Comunicados de imprensa e press kits; • Mailing lists; • Comunicações em massa aos associados; • Site web da organização; • Vídeos e imagens publicados em sites de divulgação (Youtube, Vimeo, Flickr, etc.); • Agendas e material de divulgação de eventos e programação;
Regras	Os documentos confidenciais devem: • Conter a designação “**Confidencial**”; • Indicar a lista de destinatários, nomeando o seu título ou grupo de trabalho (sem nomes);	Os documentos internos devem: • Conter a designação “**Interno**”; • Ser mantidos e distribuídos apenas dentro da organização;	Os documentos públicos devem: • Conter a designação “**ACERT - Tondela**” • Conter a URL a “http://acert.pt”; • Respeitar o estilo gráfico da organização;