SEÇÃO 11

# GESTÃO DE UM PROJETO DE ARQUIVO DIGITAL

IBERARCHIVOS IBERARQUIVOS
ARCHIVO NACIONAL COSTA RICA
UNIVERSIDAD DE COSTA RICA

# MÓDULO 7

Gestão e preservação de documentos digitais

# SEÇÃO 11

Gestão de um projeto de arquivo digital

Adaptação do Arquivo Nacional da Costa Rica
Versão 1, 2024

Este curso foi traduzido e adaptado pela Direção Geral do Arquivo Nacional da Costa Rica, em colaboração com a Seção de Arquivologia da Universidade da Costa Rica, a partir do material original de 2011 da Associação Internacional de Arquivos Francófonos, disponível online no Portal Internacional Arquivístico Francófono. Esclarece-se que podem existir variações em relação ao conteúdo original. Para acessar o material em francês, visite https://www.piaf-archives.org/se-former/module-7-gestion-et-archivage-des-documents-numeriques.

IBERARCHIVOS IBERARQUIVOS

ARCHIVO NACIONAL COSTA RICA

UNIVERSIDAD DE COSTA RICA

# Conteúdo

# Capítulo 1. Objetivo da seção

Esta seção se refere à gestão de um projeto de arquivo eletrônico que, como todos os projetos relacionados à implementação de um sistema de informação, deve ser acompanhada de uma reflexão sobre a gestão de riscos e o controle de custos, antes do real início do projeto.

Além disso, qualquer projeto de arquivo eletrônico deve ser acompanhado do desenvolvimento de uma política de arquivamento, especificando os papéis e responsabilidades dos diferentes atores e articulando-se com uma política de segurança a ser implementada, que esteja alinhada com a política geral de segurança da organização.

## GLOSSÁRIO

**Acesso à informação:** Processo de consulta e recuperação da informação arquivada.

**Administradores:** Pessoas responsáveis da administração e configuração do sistema de arquivo eletrônico.

**Aspectos Administrativos:** Os aspectos de um projeto que se relacionam com sua gestão, planejamento e controle.

**Aspectos Funcionais:** Os aspectos de um projeto que se relacionam com seu propósito ou funcionalidade previstos.

**Aspectos Técnicos:** Os aspectos de um projeto que se relacionam com sua tecnologia ou infraestrutura.

**Autoridade de arquivo:** Entidade responsável da gestão, tratamento, conservação e comunicação dos dados.

**Classificação de riscos:** O processo de categorizar riscos em função da sua probabilidade e impacto.

**Contrato ou acordo:** Documento que define o alcance dos dados a transferir/eliminar, assim como os processos de transferência e eliminação entre os diferentes atores do processo.

**Criticidade:** O nível de importância de um risco, baseado na sua probabilidade e impacto.

**Departamento de arquivos:** Unidade responsável da custódia e conservação dos dados uma vez que tenham passado sua fase ativa.

**Habilidades e Conhecimentos Comerciais:** A capacidade de compreender e aplicar princípios e práticas comerciais.

**Identificação de Riscos:** O primeiro passo na gestão de riscos, que implica identificar possíveis riscos para um projeto.

**Índice de Prioridade de Riscos (RPI):** Um valor numérico que representa a criticidade de um risco.

**Departamento de produção:** Unidade responsável pela criação e gestão dos dados durante sua fase ativa.

**Departamento de TI:** Unidade responsável por fornecer suporte técnico e tecnológico aos departamentos de produção e arquivos.

**Especialista:** Um indivíduo com experiência em um campo específico, como gestão documental ou gestão de riscos.

**Avaliação de Riscos:** O processo de avaliar a probabilidade e o impacto de cada risco identificado.

**FMEA (Análise de Modos e Efeitos de Falhas):** Um método para identificar e analisar falhas potenciais em um sistema ou processo.

**Gerente de Qualidade:** Um indivíduo responsável por garantir que a qualidade de um projeto esteja em conformidade com os padrões exigidos.

**Gestão de riscos:** O processo de identificar, avaliar e priorizar riscos em projetos de gestão documental eletrônica, com o objetivo de desenvolver e implementar estratégias de mitigação.

**Grupo de Trabalho:** Uma equipe de pessoas responsáveis por uma tarefa ou projeto específico.

**Mitigação:** As ações tomadas para reduzir a probabilidade ou o impacto de um risco.

**Modelo OAIS:** Modelo de referência para a gestão de arquivos que define os oito componentes funcionais de um sistema de arquivo eletrônico.

**Norma ISO14721:** Padrão que detalha o modelo de referência OAIS e fornece diretrizes para a implementação de sistemas de arquivamento eletrônico.

**Norma ISO20652: 2006:** Padrão abstrato de metodologia de interface de arquivamento do produtor que estabelece os princípios gerais para a interação entre o serviço de depósito e o serviço de arquivamento eletrônico.

**Política de arquivo:** Documento que estabelece as normas e procedimentos para a gestão de arquivos dentro de uma organização.

**Priorização de Riscos:** O processo de classificar riscos em função da sua criticidade.

**Usuários:** Pessoas que acessam e utilizam as informações arquivadas.

## Capítulo 2. Gestão de riscos:

A preservação de documentos digitais envolve um conjunto de ações preventivas, é antes de tudo um projeto como qualquer outro e é fundamental para garantir a eficiência e a eficácia no acesso à informação, independentemente do tempo pelo qual ela deva ser conservada.

O risco de perda de informação pode acarretar consequências graves para as pessoas, por exemplo:

- O que aconteceria com um sistema judiciário que não conseguiu conservar todos os documentos necessários para a correta realização de um julgamento?
- O que aconteceria com um sistema de saúde que perdeu o histórico de análises, exames e radiografias anteriores de um paciente?
- Se as sequelas de um acidente de trânsito aparecerem dez ou vinte anos depois desse acidente, o que se pensaria de uma companhia de seguros que não conseguiu preservar o seu prontuário?
- O que aconteceria com uma grande agência científica que realiza projetos com base em financiamento público e que não conseguiu preservar os dados resultantes desses projetos?

Portanto, é responsabilidade dos líderes dessa organização levar em consideração o problema da sustentabilidade da informação digital. Neste contexto, a gestão de riscos é fundamental porque oferece um ponto de

referência sobre o qual se baseia o desenvolvimento de acordos de serviço entre os produtores e o serviço de arquivo para a transferência de responsabilidades. Além disso, devem garantir que o compromisso do Arquivo em termos de conservação e acesso seja proporcional aos riscos que pesam sobre os documentos e devem definir as condições para uma missão contínua de monitoramento e vigilância dos riscos, que é definida no modelo OAIS como "planejamento da sustentabilidade"

Não levar em conta o problema conduz em última instância à perda de informações que podem ser valiosas, até mesmo essenciais para o funcionamento da organização. No melhor dos casos, a reconstrução das informações perdidas será necessária e exigirá recursos consideráveis.

## 2.1. Metodologia e princípios

#### Identificação e classificação de riscos

O primeiro passo crucial na gestão de riscos de projetos de gestão documental eletrônica é a identificação e classificação dos riscos potenciais. Para isso, recomenda-se estabelecer um ou mais grupos de trabalho formados por "especialistas" ou, pelo menos, por pessoas com as habilidades e conhecimentos comerciais relevantes. Esses grupos serão responsáveis por elaborar uma lista exaustiva de riscos, considerando aspectos funcionais, técnicos e administrativos. A participação de um responsável pela qualidade, quando possível, acrescentará um valor significativo em termos de rigor e eficácia do processo.

#### Avaliação de Riscos:

Uma vez identificados os riscos, deve-se proceder à sua avaliação. Para esta etapa, pode-se utilizar a abordagem FMEA (Análise dos Modos de Falha, Efeitos e Criticidade), que permite analisar os diferentes tipos de riscos, seus possíveis efeitos e seu nível de criticidade.

#### Priorização de Riscos:

A partir da avaliação de riscos, podem ser identificados os riscos prioritários. Para isso, pode-se estabelecer um limite para o Índice de Prioridade de Risco. (RPI). Os riscos que ultrapassarem esse limite exigirão um maior esforço de controle e mitigação.

## 2.2. Metodologia e princípios: segunda etapa

Por outro lado, a gestão de riscos pode ser abordada a partir da seguinte metodologia:

**Avaliação de riscos:** segundo seu grau de probabilidade (5 níveis de "improvável" a "frequente"), seu impacto (sempre 5 níveis de "insignificante" a "catastrófico") e seu grau de ocorrência no tempo (de "distante" a "iminente").

**Tomada de decisões:** Os riscos são aceitáveis? De acordo com os objetivos da organização, com o tipo de produtores e categorias de usuários, com os custos e benefícios das operações de controle de riscos, e com as obrigações legais.

**Ações** são as medidas que devem ser tomadas para conter o risco:

- que reduzem a probabilidade de um risco (escolha formatos abertos, por exemplo),
- que reduzem o impacto de um risco (por exemplo, ter um plano de backup),

- o que evita o risco (não nos responsabilizamos pelos objetos de arquivo cuja conservação seja considerada muito arriscada).

Além disso, são admissíveis outras duas categorias de ações:

- risco compartilhado: são contratadas apólices de seguro com terceiros contra violações de informação e danos imateriais, como destruição voluntária ou involuntária de dados, divulgação de informações, qualidade inadequada do programa,
- tolerância ao risco: por exemplo, decidimos assumir o risco e pagar uma compensação em vez de garantir a preservação a longo prazo de alguns dos recursos digitais que conservamos.

Uma iteração é essencial para verificar que os controles implementados não criaram outros riscos, ou para adaptar a avaliação de riscos quando o sistema é modificado, ou ainda para levar em conta a evolução dos riscos.

## COMPLEMENTO A ABORDAGEM DE ANÁLISE DE MODOS DE FALHA, EFEITOS (FMEA)

O FMEA (Análise de Modos de Falha e Efeitos) oferece uma abordagem dedutiva e exaustiva para a identificação e avaliação dos riscos que podem afetar um sistema. Este método baseia-se em três pilares fundamentais:

1. Busca das causas de falha: Realiza-se uma análise exaustiva para identificar todas as possíveis causas que poderiam provocar uma falha no sistema.
2. Busca dos mecanismos de detecção: Avaliam-se os mecanismos existentes para detectar as causas de falha antes que um impacto significativo ocorra.
3. Busca de recomendações: Propõem-se medidas para reduzir ou eliminar as causas de falha ou seu impacto no sistema.

**Classificação de riscos mediante a criticidade:**

O FMEA incorpora o conceito de criticidade para classificar e priorizar os riscos identificados. Para isso, podem ser utilizados diferentes métodos, dois dos quais são:

**1. Multiplicação da gravidade e da ocorrência:**

- Índice de gravidade: Avalia-se a severidade do impacto potencial de uma falha no sistema.
- Índice de ocorrência: Estima-se a probabilidade de ocorrência da causa de uma falha.

O Índice de Prioridade de Risco (RPI) é calculado multiplicando o índice de gravidade pelo índice de ocorrência. Um RPI superior a um limite pré-definido indica a necessidade de implementar medidas para reduzir a criticidade do risco.

**2. Multiplicação da gravidade, da ocorrência e da detecção:**

- Índice de ocorrência: Estima-se a frequência com que ocorre a causa de uma falha.
- Índice de detecção: Avalia-se a eficácia dos mecanismos existentes para detectar a causa de uma falha antes que ela se concretize.

O RPI é calculado multiplicando o índice de gravidade pelo índice de ocorrência e o índice de detecção. Um RPI elevado indica a necessidade de implementar medidas para reduzir a probabilidade de ocorrência ou melhorar a detecção do risco.

**Exemplo de aplicação:**

Consideremos o risco de degradação dos suportes em uma gravação realizada em um CD-R, seguindo as recomendações vigentes.

- Índice de gravidade: É estimado como “grave” (4) porque existe uma cópia de segurança.
- Índice de ocorrência: É estimado como “moderadamente frequente” (3) devido à vida útil limitada do CD-R (3 a 5 anos).
- Índice de detecção: Estima-se como «máximo» (5) devido à falta de mecanismos de controle.

O RPI é calculado como 60 (IPR = 4 x 3 x 5). Este valor indica que é fundamental implementar medidas para detectar a degradação dos CD-R e mitigar o risco associado.

Em resumo, o FMEA é uma ferramenta valiosa para a gestão de riscos em projetos de gestão documental eletrônica. Sua abordagem dedutiva e exaustiva permite identificar, avaliar e classificar os riscos de forma sistemática, facilitando a tomada de decisões para seu controle e mitigação.

## COMPLEMENTO O MÉTODO “ISHIKAWA”

**Definição e origem:**

O método Ishikawa, também conhecido como diagrama de espinha de peixe, é uma ferramenta gráfica utilizada na gestão da qualidade para identificar e analisar as causas de um efeito ou problema específico. A forma do diagrama, semelhante à de uma espinha de peixe, lhe dá seu nome característico.

**Objetivo:**

O objetivo principal do método Ishikawa é encontrar todas as possíveis causas que contribuem para um efeito ou problema determinado. Isso é alcançado por meio de brainstorming e da exploração de diferentes dimensões do problema.

**Funcionamento:**

O método baseia-se na criação de um diagrama onde:

- O eixo central: Representa o efeito ou problema que se deseja analisar.
- Os ramos principais: Representam as diferentes dimensões ou categorias de causas que podem estar envolvidas.
- Os sub-ramos: Representam as causas específicas dentro de cada categoria.

**As 5M de Ishikawa:**

A versão original do método, desenvolvida por Kaoru Ishikawa, propõe cinco categorias principais, conhecidas como as "5M":

- Matéria: Materiais e componentes utilizados no processo.
- Material: Equipamentos, ferramentas e instalações envolvidas.
- Método: Procedimentos, instruções e técnicas empregados.
- Meio: Ambiente de trabalho e condições ambientais.
- Mão-de-obra: Pessoas envolvidas no processo, incluindo suas habilidades e experiência.

**Adaptações e variações:**

É importante mencionar que existem variações do método Ishikawa que foram adaptadas a diferentes setores de atividade. Essas variações podem incluir outras categorias ou dimensões específicas relevantes para o setor em questão.

## 2.3. Classificação de riscos:

Os riscos podem ser classificados da seguinte maneira:

### Riscos ambientais

Os riscos ambientais são aqueles que provêm do ambiente do arquivo e podem ser divididos em três categorias:

- Riscos naturais: Eventos naturais como terremotos, inundações ou incêndios que podem afetar o arquivo.
- Riscos de segurança: Ameaças à segurança física do arquivo, como roubos ou intrusões.
- Riscos relacionados ao ambiente: inclui falhas no edifício ou no hardware necessário para os sistemas informáticos do arquivo, bem como cortes de energia ou falhas no sistema de climatização. Na sua determinação, é importante levar em conta as características particulares da localização geográfica das instalações, já que isso influencia nos riscos naturais aos quais o arquivo está exposto, assim como as particularidades do prédio já que estas determinam os riscos de segurança e das instalações.

### Riscos organizacionais

Os riscos organizacionais são aqueles que provêm da própria organização e frequentemente são subestimados ou ignorados. Entre eles encontram-se:

- Falta de habilidades: O pessoal não possui as habilidades ou os conhecimentos necessários para gerenciar o arquivo.
- Orçamento insuficiente: Não são atribuídos recursos financeiros suficientes para a operação e manutenção do arquivo.
- Processos inadequados: Os processos de gestão do arquivo não são eficientes ou não se seguem corretamente.
- Falta de liderança: Não há uma liderança clara e comprometida com a gestão do arquivo digital.

### Riscos tecnológicos

Os riscos tecnológicos estão relacionados aos suportes de gravação e aos formatos de representação utilizados no arquivo digital:

- Obsolescência tecnológica dos suportes de gravação: Os suportes de armazenamento podem se tornar obsoletos e deixar de ser compatíveis com os leitores ou reprodutores disponíveis.
- Degradação dos suportes: Os suportes de armazenamento podem deteriorar-se com o tempo e perder a informação armazenada.
- Obsolescência tecnológica dos formatos de representação: Os formatos de arquivo podem se tornar obsoletos e deixar de ser compatíveis com o software disponível.

### Riscos relacionados com o acesso

Os riscos relacionados ao acesso referem-se à capacidade dos usuários de acessar as informações do arquivo digital:

- Acessibilidade semântica: Os sistemas não conseguem compreender o objeto de informação ou carecem das informações necessárias para localizar, reconhecer e identificar esse objeto.
- Acessibilidade técnica: Os sistemas de arquivo têm dificuldades para disseminar os objetos de informação devido à ausência de metadados técnicos ou a uma estrutura inadequada, bem como à presença de sistemas de proteção ou criptografia de dados.
- Responsabilidades de acesso: Não está claro quem tem direito de acessar as informações do arquivo e como são controlados os acessos aos objetos de informação do arquivo.

## COMPLEMENTO O ENVOLVIMENTO DOS LÍDERES E AS HABILIDADES NECESSÁRIAS PARA O SUCESSO DO ARQUIVO DIGITAL

***O envolvimento dos líderes e as habilidades necessárias para o sucesso do arquivo digital***

**O arquivo digital tornou-se uma atividade fundamental**, situada na interseção entre a arquivística e a tecnologia da informação. O sucesso desse tipo de projeto depende, em grande medida, da capacidade dos diferentes atores de trabalhar em conjunto, bem como da existência de perfis profissionais que combinem habilidades em ambas as áreas.

**Dada a diversidade de competências requeridas** para a construção do projeto (arquivística, informática, jurídica, qualidade) e a ausência, na maioria dos casos, de uma estrutura ou serviço especializado nessa área, **é crucial que a direção da organização se envolva de forma ativa.** Isso pode ser feito por meio da nomeação de um grupo de trabalho ou da criação explícita de um projeto dedicado ao arquivo digital.

**Essa decisão tem vários benefícios:**

- **Visibiliza a importância do projeto** e demonstra o compromisso da direção com ele.
- **Permite mostrar a transversalidade do problema** aos diferentes atores internos e externos.
- **Facilita a obtenção de apoio** dos serviços e das pessoas que serão afetados pelas mudanças decorrentes da implementação do arquivo digital.

**Além do envolvimento da direção, é necessário contar com equipes de projeto e estruturas permanentes** que estejam totalmente dedicadas ao arquivo digital. Essas equipes devem possuir as diversas habilidades requeridas para o projeto, sendo importante que essas diferentes competências se apoiem em uma compreensão comum dos problemas a serem resolvidos.

**O papel da direção é decisivo** para o sucesso do projeto. A direção deve demonstrar seu apoio ao projeto de forma clara e visível, além de estabelecer objetivos claros que sejam conhecidos por todas as partes interessadas.

## 2.4. Conclusões sobre a gestão de riscos

A gestão de riscos é uma ferramenta fundamental para a preservação de objetos digitais. Permite utilizar os dados dos riscos identificados para gerar um painel de controle que facilite a tomada de decisões e o planejamento de ações.

Este painel de controle, também conhecido como “plano de preservação digital”, oferece as seguintes vantagens:

- Planejamento de revisões: Permite monitorar a evolução dos dados, das aplicações e dos meios de armazenamento. Isso garante que as opções técnicas e organizativas escolhidas continuem sendo válidas e que sua qualidade seja boa. As revisões geram relatórios que ativam alertas em caso de detectar uma situação anormal.
- Antecipação de alertas e soluções: O sistema pode detectar problemas de forma precoce e emitir um sinal de alerta. Isso permite ativar um processo de resolução de problemas predefinido, como um plano de emergência.
- Determinação de riscos específicos: Permite identificar os riscos específicos de cada tipo de objeto digital e ponderar a avaliação de riscos de acordo com as suas particularidades técnicas ou de outro tipo.

O sistema de gestão de riscos também pode ser auditado para obter uma certificação ou para priorizar ações. A gestão de riscos proporciona uma visão geral de todas as ações de conservação que estão sendo realizados nos objetos digitais.

Em resumo, a gestão de riscos é uma ferramenta essencial para a preservação digital. Permite às organizações:

- Identificar e avaliar os riscos que ameaçam seus objetos digitais.
- Planejar e executar ações para mitigar esses riscos.
- Monitorar a eficácia das medidas de preservação.
- Tomar decisões informadas sobre a gestão de seus arquivos digitais.

## Capítulo 3. Controle de custos

Qualquer projeto de implementação de um Arquivo Digital deve cumprir com os requisitos metodológicos de qualquer projeto. Isso implica identificar as etapas e as condições necessárias para passar de uma fase à seguinte.

Antes de entrar em detalhes na análise, é necessário estabelecer alguns elementos preliminares:

- A entidade de Gestão de Arquivos deve estar claramente identificada. Essa entidade é a que define o mandato do Arquivo e atribui os recursos necessários para cumprir os objetivos decorrentes desse mandato.
- O mandato concedido ao Arquivo pela Direção deve estar claramente explicado. Isso inclui:
    - Quem são os produtores de informação.
    - Quem são os usuários do Arquivo.
    - Que serviços será oferecido aos usuários.
    - Quais são os objetos a serem arquivados.
    - Qual é o período de conservação dos objetos.
    - Qual é o valor probatório dos objetos.
- Os distintos aspectos regulatórios e legais devem estar explicados por escrito.
- O Arquivo deve ter recursos quantificados. Isso inclui:
    - Recursos humanos
    - Recursos financeiros.
    - Recursos tecnológicos.
- O Arquivo deve ter uma política de arquivo. Esta política deve definir:
    - Os critérios de seleção dos documentos a serem arquivados.
    - Os procedimentos de arquivo.
    - Os métodos de acesso e consulta dos documentos.
- O Arquivo deve desenvolver um plano de reversibilidade. Esse plano deve definir como serão extraídos todos os dados e metadados do Arquivo em caso de que o Arquivo tenha que cessar suas atividades.

Estabelecer estes elementos preliminares é essencial para controlar os custos do projeto de implementação do Arquivo Digital. Ao ter uma compreensão clara dos requisitos do projeto, é possível realizar um planejamento preciso e eficiente dos recursos necessários.

## 3.1. Avaliação de custos

A avaliação dos custos do arquivo digital é um exercício complexo, porém fundamental, tanto no presente como no futuro. O desenvolvimento exponencial das tecnologias digitais gerou um crescimento exponencial nos volumes de dados que precisam ser arquivados a um ritmo muito mais acelerado do que os arquivos tradicionais em papel.

É insustentável para a entidade responsável pelo arquivamento ou para seu cliente embarcar em uma espiral de custos sem perspectivas de estabilidade ou redução. Torna-se indispensável não apenas estimar os custos do arquivamento, mas também demonstrar a capacidade de operar com custos estáveis, mesmo diante do aumento contínuo dos volumes de informação a serem arquivados, excetuando-se os casos de mudanças significativas em seu mandato.

Por exemplo, a NASA, com sua vasta experiência em processamento e arquivamento de dados, desenvolveu uma ferramenta para avaliar os custos de desenvolver, operar e manter sistemas para processar e arquivar dados científicos, que é distribuída como software gratuito e está disponível no seguinte link: https://opensource.gsfc.nasa.gov/ projects/CET/index.php

### COMPLEMENTO MODELO DE CUSTO PARA A PRESERVAÇÃO DIGITAL

O Modelo de Custo para a Preservação Digital (CMDP) é uma ferramenta que permite às instituições estimar os custos associados à preservação digital a longo prazo. O CMDP baseia-se em uma série de fatores, incluindo:

- O tipo de objetos digitais que serão preservados: Isso inclui formatos de arquivo, tamanho e complexidade.
- As estratégias de preservação que serão utilizadas: Isso inclui a replicação, a migração e a emulação.
- A infraestrutura de TI utilizada: Isso inclui hardware, software e armazenamento.
- Os recursos humanos necessários: Isso inclui pessoal com as habilidades e conhecimentos necessários para a preservação digital.

O CMDP pode ser utilizado para:

- Planejar e orçar projetos de preservação digital.
- Comparar os custos de diferentes estratégias de preservação.
- Justificar o investimento em preservação digital às partes interessadas.

Pode ser consultada informação adicional sobre este modelo nos seguintes links:

- https://www.4cproject.eu/summary-of-cost-models/16-community-resources/outputs-and-delivera-bles/108-cost-model-for-digital-preservation-cmdp/
- https://coptr.digipres.org/index.php/CMDP_(Cost_Model_for_Digital_Preservation)

## 3.2. O estudo realizado para os serviços públicos de arquivo

Em um estudo de custos, é fundamental analisar o impacto do modelo organizacional selecionado, especialmente no que diz respeito à compartilhamento de recursos.

Essa influência tem sido demonstrada em estudos realizados, por exemplo, no âmbito dos serviços públicos de arquivo.

Dessa forma, pode-se citar um estudo sobre o desenvolvimento de plataformas de arquivo eletrônico para serviços públicos de arquivo, realizado por Parker Williborg a pedido da Direção de Arquivos da França, onde se aborda a questão da avaliação de custos no setor público.

Em particular, analisa o impacto do modelo organizacional escolhido e, portanto, o impacto do compartilhamento de recursos nos custos. Foram estudados cinco cenários, desde uma plataforma local e isolada até uma plataforma nacional amplamente compartilhada:

- Cenário 1: uma plataforma dedicada a um único serviço de produtor, que armazena seu próprio acervo ou possui um serviço de arquivamento interno (por exemplo, um grande município, um conselho regional).
- Cenário 2: uma plataforma dedicada a um conjunto de serviços locais de produtores (como serviços de arquivo departamentais ou alguns serviços de arquivos municipais de grande porte).
- Cenário 3: uma plataforma nacional dedicada a todos os serviços centrais e descentralizados no âmbito de um mesmo ministério.
- Cenário 4: uma plataforma nacional dedicada a um conjunto de comunidades do mesmo tipo (conselhos regionais, conselhos estaduais).
- Cenário 5: uma plataforma nacional para todas as administrações do governo central (Arquivos Nacionais).

### EXEMPLO APLICAÇÃO DO ESTUDO

**Estimativa de volumes para os próximos 10 anos**

A estimativa de volumes para os próximos 10 anos baseia-se na identificação de fontes candidatas para o arquivamento eletrônico. Foi considerada a retenção de todos os dados duplicados para garantir a integridade da informação arquivada.

**Estimativa de recursos humanos**

A estimativa dos recursos humanos necessários baseou-se em uma análise detalhada das funcionalidades da plataforma, divididas por processo principal (preparação e suporte de pagamentos, armazenamento, gestão de dados descritivos, restituição) e por funções transversais (administração da plataforma, pilotagem, monitoramento tecnológico e jurídico, desenvolvimento e projetos de migração).

A seguir, as tarefas foram detalhadas com a determinação de um tempo médio por tarefa e um custo horário dos agentes. Foram elaboradas diferentes estimativas com base na escolha de maior ou menor automação dos processos, no uso de redes ou mídias removíveis para transmissões, na instalação de plataformas manuais (suportes em prateleiras) ou automatizadas, etc.

**Avaliação de custos iniciais e custos anuais**

O funcionamento da plataforma de arquivamento eletrônico baseou-se na premissa de desenvolvimento em nível nacional, utilizando pacotes de software comerciais (que exigiriam um trabalho significativo de integração) e uma solução genérica seguindo estes passos:

1. Desenvolvimento
2. Implantação piloto
3. Generalização da solução

Esse enfoque conduziu ao desenvolvimento da plataforma piloto Pilze.

Partindo da disponibilidade da plataforma genérica, foram estimados os custos específicos de cada plataforma implementada. Esses custos incluem, por um lado, os custos iniciais de aquisição da plataforma operacional, instalação da solução genérica adequada e custos internos de implantação junto aos departamentos produtores. Por outro lado, foram considerados os custos operacionais anuais, que variam conforme o processo (pagamento de licenças, custo da gestão de armazenamento, custo de devoluções e consultas, custo de aplicação e manutenção técnica, custo das funções transversais).

**Análise de cenários e comparação de custos por terabyte**

Foram analisados cenários e comparação de custos por terabyte Os resultados revelam que, à medida que aumentam os volumes arquivados, as economias de escala são consideráveis:

- Os custos por terabyte são consistentemente mais de vinte vezes maiores entre o primeiro cenário (plataforma de arquivamento dedicada a um único serviço produtor) e o último (plataforma nacional), tanto para custos externos iniciais quanto operacionais. Portanto, recomenda-se incentivar o uso de plataformas de maior porte.
- Os custos internos mais significativos estão relacionados ao início de um processo de arquivamento com um novo serviço produtor (novo produtor/nova aplicação). Esses custos são particularmente elevados para as categorias A no início e as categorias B para a operação. Isso se aplica tanto ao serviço de arquivamento quanto ao produtor, que deverá adaptar sua aplicação para a transferência no formato definido pelo esquema de transferência XML para a plataforma de arquivamento.

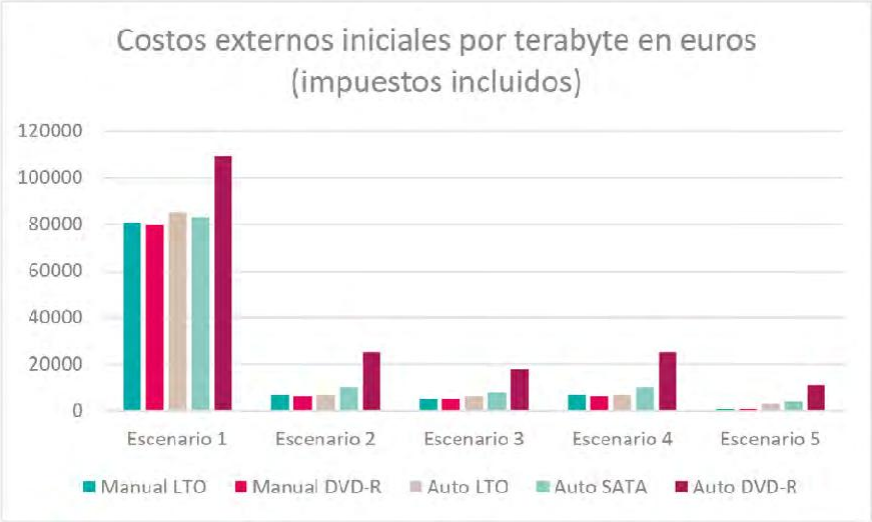
**Recomendações**

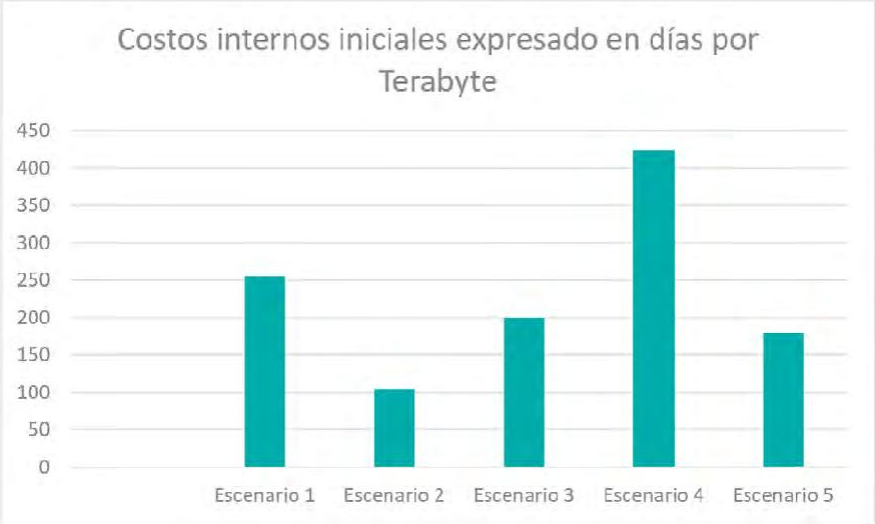
Com base nos resultados do estudo, recomenda-se:

- Priorizar os pagamentos de grande volume para otimizar os custos.
- Limitar o número de diferentes serviços de produção, caso não se disponha de recursos humanos suficientes.

- Fortalecer o nível central (Direção de Arquivos da França) para fornecer assistência na modelagem de pagamentos por categorias principais de documentos, que estão presentes em todos os sites (exemplo: licitações públicas).

Dessa forma, o gráfico a seguir apresenta os custos iniciais em função dos cenários listados anteriormente, com a implementação de diferentes tipos de armazenamento:



## Caso de um único serviço produtor que garante seu próprio arquivamento

| | PLATAFORMA MANUAL /LTO | | |
|---|---|---|---|
| | **Custos externos (euros com IVA)** | **Custo por dia do serviço para um Agente categoria A** | **Custo por dia do serviço para um Agente categoria B** |
| **Custos iniciais** | | | |
| Aquisição da plataforma Operação | 39 468,00 | | |
| Instalação e desenvolvimento no site | 42 338,40 | 50 | |
| Início dos serviços produtores | | 10 | |
| Início das aplicações fonte | | 200 | |
| **Total** | **81 806,40** | **260** | **0** |
| **Custo por Terabyte** | **81 806,40** | **260** | **0** |
| **Custo operacional anual** | | | |
| Pagamentos | | | 27,58 |
| Armazenamento | 388,7 | | 0,20 |
| Consulta/restituição | 299 | | 10,15 |
| manutenção das aplicações | 8 467,68 | 10 | |
| Operação e manutenção técnico | 10 405,20 | | 40 |
| Funções transversais1 | | 35 | 95 |
| Encargos variáveis de administração2 | | 21,8 | |
| **Total** | **19 560,58** | **66,8** | **172,96** |
| **Custo por Terabyte** | **19 560,58** | **66,8** | **172,96** |

## Caso de uma plataforma nacional para todos os órgãos do governo central

| | PLATAFORMA AUTOMATIZADA /LTO | | |
|---|---|---|---|
| | **Custos externos (euros com IVA)** | **Custo por dia do serviço para um Agente categoria A** | **Custo por dia do serviço para um Agente categoria B** |
| **Custos iniciais** | | | |
| Aquisição da plataforma Operação | 222 755,00 | | |
| Instalação e desenvolvimento no site | 42 338,40 | 50 | |

1 Excluídos os custos variáveis de Administração.

2 igual a 10% do quadro de pessoal (agentes das categorias A e B)

| | PLATAFORMA AUTOMATIZADA /LTO | | |
|---|---|---|---|
| | **Custos externos (euros com IVA)** | **Custo por dia do serviço para um Agente categoria A** | **Custo por dia do serviço para um Agente categoria B** |
| Início dos serviços produtores | | 200 | |
| Início das aplicações fonte | | 1600 | |
| **Total** | **265 093,40** | **1850** | **0** |
| **Custo por Terabyte** | **2 650,93** | **18,5** | **0** |
| **Custo operacional anual** | | | |
| Pagamentos | | | 220,6 |
| Armazenamento | 38870 | | |
| Consulta/restituição | 5980 | | 78 |
| manutenção das aplicações | 8 467,68 | 10 | |
| Operação e manutenção técnico | 47 062,60 | | 40 |
| Funções transversais3 | | 35 | 190 |
| Encargos variáveis de administração4 | | 57,36 | |
| **Total** | **100 380,28** | **102,36** | **528,6** |
| **Custo por Terabyte** | **1 003,80** | **1,02** | **5,29** |

## 3.3. Fatores a serem considerados no cálculo de custos

**Quadro resumo dos fatores de custo a serem considerados.**

| **Aspectos a serem considerados** | **Recursos humanos** | | **Infraestrutura: hardware, locais, redes** | | **Validação e desenvolvimento de software** | |
|---|---|---|---|---|---|---|
| | Implementação | Operação | Implementação | Operação | Implementação | Operação |
| Quantidade de serviço produtores (número de protocolos de pagamento, número de contatos) | Alto | Alto | | | | |

3 Excluídos os custos variáveis de Administração.

4 igual a 10% do quadro de pessoal (agentes das categorias A e B)

| **Aspectos a serem considerados** | **Recursos humanos** | | **Infraestrutura: hardware, locais, redes** | | **Validação e desenvolvimento de software** | |
|---|---|---|---|---|---|---|
| | Implementação | Operação | Implementação | Operação | Implementação | Operação |
| Natureza das relações com os produtores: é possível impor formatos de arquivo ou o Arquivo será obrigado a migrar formatos desde o princípio, fornecimento completo de metadados ou não? | Alto | | | | Alto | |
| Complexidade do conteúdo (Associação de elementos documentais com objetos de informação arquivados) | Alto | Alto | | | | |
| Número e complexidade dos formatos de dados. | Alto | | | | Alto | Alto |
| Proporção de documentos sujeitos a limitações de valor probatório (que implicam o uso sistemático de assinaturas eletrônicas, cálculos de impressões digitais e carimbo de tempo) | Alto | | Alto | | Alto | |
| Baixo nível de automatização de pagamentos (possível existência de operações manuais sistemáticas) | | Alto | | | | |
| Alto nível de automatização de pagamentos | | | | | Alto | Alto |
| Disponibilidade de componentes de software reutilizáveis | | | | | Alto | |
| Alto volume (impacto na capacidade dos recursos de armazenamento, no monitoramento das operações e sua renovação periódica como parte das migrações de suporte) | | Médio | Alto | Alto | | |
| Granularidade dos objetos (a gestão de um grande número de objetos não deixa de ter consequências sobre as limitações que pesam sobre a base de dados) | | | Alto | | Médio | |
| Requisitos de segurança, criticidade e confidencialidade dos dados | Alto | | Alto | | Alto | |

| **Aspectos a serem considerados** | **Recursos humanos** | | **Infraestrutura: hardware, locais, redes** | | **Validação e desenvolvimento de software** | |
|---|---|---|---|---|---|---|
| | Implementação | Operação | Implementação | Operação | Implementação | Operação |
| Requisitos de continuidade do serviço: taxas de indisponibilidade aceitáveis. Um serviço aberto as 24 horas do dia com um baixo índice de indisponibilidade deve contar com recursos redundantes e um sistema de vigilância | | Alto | Alto | Alto | Médio | Médio |
| Número de usuários que podem consultar o serviço em paralelo | | | Alto | | | |
| Requisitos de nível de serviço para que os usuários acessem os documentos de forma mais ou menos rápida, interface e meios sofisticados de busca e recuperação. | | | Alto | | Alto | |
| Atendimento ao cliente (gestão de usuários e seus direitos de acesso) | | Alto | | | | Médio a Alto |
| Frequência de auditorias de pacotes pagos e pacotes arquivados | | Alto | | | | |
| Suporte gratuito aos usuários (se o suporte for pago, este constituirá uma fonte de recursos para o Arquivo) | | Alto | | | | |
| Acompanhamento tecnológico, acompanhamento da evolução das normas, necessidades dos usuários, etc. | | Alto | | | | |

## 3.4. Formas de reduzir custos

As primeiras vias a serem examinadas são internas ao Arquivo e se concentram em sua organização, funcionamento, equipamento e racionalização de suas atividades.

Quanto à redução de custos, as possibilidades de compartilhar despesas com outros Arquivos ou outros departamentos da organização são diversas e numerosas. O objetivo principal é distribuir os custos da maneira mais ampla possível, considerando as seguintes estratégias:

1. Reutilização da infraestrutura de TI existente na organização:

- Aproveitar os recursos de informática já disponíveis dentro da organização para reduzir a necessidade de investimentos adicionais

2. Compartilhar infraestrutura de armazenamento:

- A experiência demonstra que configurar e administrar uma infraestrutura de armazenamento requer habilidades e recursos humanos semelhantes, independentemente da quantidade de dados armazenados (50 TB ou 500 TB).
- Explorar acordos de reciprocidade com outros Arquivos para compartilhar infraestrutura de armazenamento, garantindo a segurança e a redundância dos dados digitais em dois locais geograficamente distantes.

3. Desenvolvimento de sistemas de software genéricos adaptáveis a múltiplos contextos:

- Implementar uma abordagem modular no desenvolvimento de software, permitindo a reutilização de componentes e a adaptação a diferentes necessidades dentro do mesmo domínio.
- Um exemplo dessa abordagem é um serviço de arquivos que recebe arquivos de vários produtores, mas utiliza uma única ferramenta de busca para todos os acervos arquivados, independentemente dos campos administrativos.

4. Reutilização de componentes de software da aplicação de arquivo:

Fomentar a reutilização de componentes de software gratuitos ou comerciais para reduzir custos de desenvolvimento e otimizar recursos.

Em um campo específico, como o dos serviços de arquivos públicos, arquivos científicos ou otros, 90% das necessidades de software podem ser comuns.

Projetar software considerando a reutilização para gerar interesse nas empresas de software e otimizar custos para os Arquivos.

Na área de pagamento, devem ser considerados dois pontos importantes:

1. Limites de pagamento vinculados ao arquivo de documentos:

- Considerar as limitações de pagamento no momento da criação do documento ou quando o documento é bloqueado e deixa de ser modificável.
- Implementar mecanismos para gerenciar pagamentos de maneira eficiente e segura.

2. Máxima automatização do processo de transferência e criação de pacotes de informação arquivados:

- Automatizar o processo de transferência de arquivos, assegurando a padronização dos pacotes SIP (Standard Information Package).
- Automatizar a criação de pacotes de informação arquivados para otimizar o armazenamento e a gestão de dados.

O trabalho de definição de padrões não deveria ser responsabilidade de apenas um Arquivo.

- É recomendável reutilizar os padrões existentes e compartilhar a tarefa de redação de novos padrões com outros Arquivos quando surgirem novas necessidades.
- A colaboração entre Arquivos permitirá estabelecer padrões eficientes e adequados para a gestão de arquivos digitais.

**EXEMPLO**

A Direção de Arquivos da França e a Direção Geral de Modernização do Estado disponibilizam a todos os serviços públicos de arquivos modelos de descrição, não componentes de software. Esses modelos cumprem o padrão de "intercâmbio de dados para o arquivo" e são essenciais para desenvolver transferências. Os modelos estão disponíveis para uma categoria de arquivos que podem ser encontrados em todo o território nacional.

# Capítulo 4. Desenvolvimento de uma política de arquivo

Com a tecnologia digital, os riscos de litígio tornam-se mais significativos: determinação dos papéis e responsabilidades dos diversos atores que intervêm ao longo do ciclo de vida do documento, problemas de integridade (como provar que o documento original não foi modificado?), Problemas de conversão de formato (como demonstrar que o documento convertido não perdeu a funcionalidade original), problemas de mídias defeituosas que danificaram ou fizeram desaparecer os dados, problemas de direitos de acesso, por isso, é necessário especificar, no âmbito de uma política de arquivo, todos os elementos que participarão na implementação do processo adequado de arquivamento para assegurar que um documento foi devidamente integrado, controlado, conservado, gerenciado e consultado ao longo de seu ciclo de vida.

## 4.1. Objetivos da política ou carta de arquivo

A ação do arquivista será tanto mais eficaz quanto existir uma carta de arquivo dentro da organização, validada no mais alto nível e válida para todas as informações recebidas ou produzidas na organização, independentemente de sua forma. Por tanto, a carta ou política de arquivo deve ser aplicada a toda a produção, com especificidades obviamente vinculadas à produção digital.

A carta ou política de arquivo estabelecerá as boas práticas que sustentam a gestão arquivística. Definirá o marco legal vigente, identificará os atores envolvidos e detalhará suas respectivas obrigações e responsabilidades. Nesse sentido, a política de arquivo estabelece os requisitos mínimos, em termos legais, funcionais, operacionais, técnicos e de segurança, que um arquivo eletrônico deve cumprir para ser considerado confiável. Esses requisitos baseiam-se nas restrições "padrão" que devem ser implementadas e que são listadas a seguir:

Restrições materiais

- Identificação e autenticação da origem dos documentos arquivados.
- Integridade dos arquivos.
- Inteligibilidade e legibilidade dos arquivos.
- Vida útil dos arquivos.
- Rastreabilidade das diversas operações (criação, modificação, consulta, eliminação).
- Disponibilidade e acessibilidade dos arquivos

Esta carta ou política constitui um marco de referência fundamental para garantir a confiabilidade de um arquivo eletrônico. Uma matriz de auditoria composta por seus diferentes capítulos permite ao auditor avaliar a confiabilidade de um serviço de arquivo eletrônico A auditoria deve verificar, em particular, que os processos para aplicar a política de arquivo foram definidos e que esses processos são efetivamente aplicados. A pessoa responsável pela implementação da política de arquivo deve estar claramente designada e ser conhecida pelas partes interessadas, que podem solicitar sua assistência para fins informativos e operacionais.

A carta de arquivo é um documento de alto nível que deve ser complementado por documentos mais detalhados, que descrevam sua implementação em termos de organização, processos e procedimentos.

## 4.2. Responsabilidades e obrigações das distintas partes

A autoridade arquivística é a entidade responsável pelo arquivo (gestão, tratamento, preservação e comunicação dos dados).

De fato, ao longo do ciclo de vida de um documento, pode haver várias autoridades arquivísticas sucessivas: no setor público, o serviço do produtor enquanto o arquivo estiver “ativo”; em seguida, um serviço de arquivo intermediário para a “idade intermediária”; e, por fim, um serviço de arquivo definitivo para a “idade permanente”; ou o produtor durante as idades ativa e intermediária, e o serviço de arquivo para a idade permanente. A transferência antecipada de dados para o serviço de arquivo antes do término do período intermediário não altera essa distribuição de responsabilidades.

Por sua vez, o departamento de TI terá um papel de operador que exercerá inicialmente para o departamento de produção e, em um segundo momento, para o departamento de arquivos, quando este se tornar a Autoridade Arquivística.

O contrato ou acordo firmado entre os diferentes atores do processo (departamento de produção, departamento de arquivos, departamento de TI) define o escopo dos dados a serem transferidos/eliminados, bem como os processos de transferência e eliminação.

A análise geral das interfaces e interações entre o serviço de depósito e o serviço de arquivo eletrônico é o tema da norma ISO20652: 2006 “Padrão abstrato de metodologia de interface de arquivamento do produtor”. Este padrão é estudado na parte 5 sobre o modelo OAIS e os padrões derivados, e pode ser analisado em detalhe na norma ISO 14721 “Sistemas de transferência de dados e informações espaciais. Sistema aberto de informação de arquivo (OAIS). Modelo de referência”.

Finalmente, os demais atores do processo (administradores, usuários) terão um número de obrigações e responsabilidades a serem definidas no âmbito desta política de arquivo, especialmente no que diz respeito ao acesso à informação.

## 4.3. Obrigações do serviço produtor

O serviço produtor deve garantir o seguinte:

- Gestão do sistema de informação:
    - Alimentar e atualizar o sistema de informação.
    - Informar ao departamento de informática sobre duplicatas, erros e arquivos vazios.
- Integração do ciclo de vida dos dados digitais:
    - Integrar o ciclo de vida dos dados digitais no sistema de informação.
- Transferência de arquivos fechados:
    - Se existir um módulo de arquivo interno ou uma base de dados de arquivo intermediária, transferir os arquivos fechados e gerar um relatório dessa base de dados em caso de dados pessoais.
    - Manter a integridade dos dados nesta base de dados.
- Aspectos volumétricos e calendário de traslados:
    - Proporcionar informação sobre os aspectos volumétricos dos traslados ao serviço de arquivos.
    - Se for o caso, fornecer um calendário provisório das futuras traslados.
- Meios e protocolos de transferência:
    - Definir os meios que podem ser utilizados para as transferências que não utilizem uma rede informática.
    - Para as transmissões em rede, definir os protocolos que serão utilizados.
- Formatos de codificação de dados:
    - Definir os formatos de codificação de dados que aceita o serviço de arquivos.
    - Se o formato original dos arquivos não permite garantir uma boa continuidade da informação, definir os métodos de conversão de formatos que o serviço de arquivos deseja realizar na chegada dos arquivos transferidos.
- Informação sobre os arquivos transferidos:
    - Fornecer todas as informações relativas à natureza e duração dos arquivos transferidos, assim como sua possível confidencialidade e acesso restrito.
    - O departamento de produtores é responsável pela veracidade dessas informações e pela sua correta transmissão.
- Cumprimento dos requisitos técnicos:
    - Cumprir com os requisitos técnicos definidos pela Autoridade Arquivística.

    - Em particular, cumprir com um formato de intercâmbio de dados e garantir que os meios e os arquivos que contêm estejam em perfeito estado e livres de vírus ou outras anomalias que possam impactar a correta execução da política de arquivo.
- Verificação de assinaturas digitais:
    - No caso de documentos assinados digitalmente que serão transferidos para o serviço de arquivos, verificar a assinatura antes da transferência prevista.
    - Registrar os resultados dessa verificação nos metadados dos documentos em questão.

Durante a transferência, deve-se gerar as impressões digitais dos arquivos transferidos, a fim de permitir que a Autoridade Arquivística verifique a integridade destes ao serem recebidos.

## 4.4. Obrigações do departamento de Tecnologias da Informação

Na qualidade de operador de arquivo, as unidades de TI devem comprometer-se com o seguinte:

- Executar as operações de transferência ou eliminação de dados digitais em nome da Autoridade Arquivística.
- Garantir a eliminação física dos dados digitais uma vez finalizado seu período de utilidade administrativa, mediante aprovação prévia para a eliminação por parte do serviço de arquivos.
- Emitir um relatório detalhado sobre a destruição dos dados eliminados.
- Garantir um acesso seguro aos usuários do Arquivo mediante a implementação de uma gestão de autorizações adequada e a provisão de meios de acesso dimensionados de acordo com as necessidades e os recursos disponíveis.
- Assegurar o desenvolvimento e implementação das mudanças necessários.
- Administrar e operar os sistemas de maneira eficiente e eficaz.
- Garantir a confiabilidade operacional dos sistemas mediante o estabelecimento de um plano de recuperação ou continuidade do negócio de acordo com o nível de qualidade de serviço exigido pelos usuários.
- Proteger a integridade dos objetos digitais por meio de um armazenamento seguro de dados digitais que inclua redundância, replicação em vários locais remotos, monitoramento constante dos meios e migração periódica desses meios.
- Manter-se na vanguarda da evolução tecnológica da infraestrutura.
- Implementar as operações de migração solicitadas pelo serviço de arquivos, incluindo prototipagem, testes exaustivos e acompanhamento da execução.

## 4.5. Obrigações do serviço de arquivo

O serviço de arquivo é responsável por:

- Definir, em colaboração com o departamento de produção, as regras relativas ao ciclo de vida dos dados no sistema de informação.
- Examinar as solicitações de visto de eliminação que lhe são dirigidos.

- Receber, no formato de intercâmbio especificado, os arquivos transferidos e verificá-los para sua validação ou rejeição. Se o controle for satisfatório, gerar uma mensagem de aceitação da transferência que, potencialmente, possa ser coberta por uma assinatura digital. Essa mensagem deve indicar a assunção de responsabilidade e, portanto, a responsabilidade da Autoridade Arquivística pelos arquivos transferidos.
- Aplicar, em caso de transferência antes da expiração do período de utilidade administrativa (PUA), o período de conservação adequado para os arquivos em questão, de acordo com as instruções fornecidas pelo departamento de produção.
- Definir as regras que permitem o armazenamento de dados a longo prazo, que deve implementar o departamento de TI.
- Verificar todos os acessos ao serviço de arquivos, tanto físicos quanto lógicos, internos e externos, de acordo com os direitos de cada uma das partes envolvidas.
- Permitir o acesso aos arquivos processados apenas às pessoas autorizadas.
- Solicitar ao serviço de produtores a autorização para qualquer pedido de comunicação dos arquivos em questão, desde que os prazos de livre comunicação não tenham expirado.
- Exigir a assinatura de um acordo de segredo e confidencialidade por parte de todo o pessoal externo e dos subcontratados.
- Tomar uma série de medidas assim que transferir os arquivos pelos quais é responsável preservar para outra autoridade arquivística (por exemplo, de um serviço de arquivos intermediário para um serviço de arquivos definitivo).

## COMPLEMENTO

***Exemplos de políticas de arquivo***

Sobre o desenvolvimento de políticas de arquivo, pode-se consultar o modelo desenvolvido pelo governo da Espanha, disponível no seguinte link: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Politica-de-gestion-de-documentos-electronicos.html

Da mesma forma, pode-se consultar o Guia de Implementação Gerencial – Política de gestão de documentos e arquivos, que faz parte do Modelo de Gestão de Documentos e Administração de Arquivos (MGD) para a Rede de Transparência e Acesso à Informação (RTA) e que está disponível no seguinte link: http://mgd.redrta.org/guia-de-implementacion-gerencial-politica-de-gestion-de-documentos-y-archivos/mgd/2015-01-21/124946.html

***Modelos de requisitos***

Por outro lado, pode-se consultar o modelo proposto, o modelo MoReq2010, disponível no seguinte link:https://moreq.info/

Além disso, sobre os padrões e aplicações baseadas no modelo de referência OAIS recomenda-se aprofundar os trabalhos desenvolvidos pelo projeto E-ARK e mantidos pela Digital Information LifeCycle Interoperability Standards Board (DILCIS Board), todas as informações relacionadas a essa iniciativa estão disponíveis no seguinte link: https://dilcis.eu/

# Capítulo 5. Política de segurança a ser implementada

A gestão de arquivos digitais envolve a captura, o armazenamento, a preservação, o acesso e a eliminação de dados eletrônicos. A segurança dos arquivos digitais é fundamental para garantir a confidencialidade, a integridade e a disponibilidade da informação, assim como para cumprir as regulamentações legais e normativas aplicáveis.

Nesse contexto, a Autoridade Arquivística deve estabelecer e implementar uma Política de Segurança de Sistemas de Informação (PSSI) alinhada aos padrões e regulamentações aplicáveis à organização ou instituição à qual pertence. Essa política de segurança deve abordar os aspectos específicos da gestão de arquivos e garantir a proteção adequada dos dados e dos sistemas arquivísticos.

Da mesma forma, a Autoridade Arquivística mantém a responsabilidade geral pela segurança de todos os processos de arquivamento, mesmo que determinadas funções desses processos sejam delegadas a componentes externos. É responsabilidade da Autoridade de Arquivo:

- Estabelecer e implementar uma PSSI integral que abranja todos os aspectos da gestão de arquivos. Isso inclui a definição de papéis e responsabilidades em matéria de segurança, a identificação e avaliação de riscos, a implementação de medidas de segurança técnicas e não técnicas, a gestão de incidentes de segurança e a realização de auditorias periódicas.
- Garantir o cumprimento dos requisitos de segurança estabelecidos na PSSI por todos os componentes internos e externos envolvidos nos processos de arquivamento. Isso pode exigir a negociação de acordos de segurança com fornecedores externos e a implementação de mecanismos de controle para garantir o cumprimento dos requisitos de segurança.
- Implementar mecanismos de monitoramento e controle para garantir a aplicação efetiva da PSSI. Isso pode incluir a instalação de ferramentas de monitoramento de segurança, a realização de testes de penetração e a realização de auditorias internas de segurança.
- Incentivar a participação da direção da Autoridade Arquivística na definição e implementação da política de segurança da informação. O compromisso da direção é essencial para garantir a alocação adequada de recursos e a criação de uma cultura de segurança dentro da organização.
- Realizar análise de riscos periódicos para identificar e avaliar os riscos potenciais que possam afetar a segurança dos arquivos e sistemas arquivísticos. A análise de riscos deve considerar ameaças internas e externas, assim como as vulnerabilidades dos sistemas e processos de arquivo.
- Definir objetivos de segurança específicos e mensuráveis para mitigar os riscos identificados na análise de riscos. Os objetivos de segurança devem ser realistas, alcançáveis e alinhados com as estratégias de segurança da organização.
- Implementar medidas de segurança técnicas e não técnicas adequadas para cumprir com os objetivos de segurança estabelecidos. As medidas de segurança técnicas podem incluir firewalls, sistemas de detecção de intrusões, softwares antivírus e antimalware, criptografia de dados e mecanismos de backup. As medidas de segurança não técnicas podem incluir capacitação em segurança para o pessoal, procedimentos de segurança documentados, gestão de riscos e vulnerabilidades, auditorias de segurança e monitoramento contínuo de sistemas e redes.

- Estabelecer um nível mínimo de garantia de segurança para os sistemas de TI da Autoridade Arquivística. Esse nível mínimo deve considerar os aspectos de confidencialidade, integridade, disponibilidade, não repúdio e autenticidade da informação arquivística.
- Documentar a PSSI e mantê-la atualizada regularmente. A PSSI deve ser um documento claro, conciso e fácil de entender que esteja disponível para todas as partes interessadas. A PSSI deve ser revisada e atualizada periodicamente para refletir as mudanças no ambiente de segurança e nas necessidades da organização.
- Análise de riscos e objetivos de segurança. A Autoridade Arquivística deve realizar análise de riscos periódica para identificar e avaliar os riscos potenciais que possam afetar a segurança dos arquivos e sistemas arquivísticos. Esta análise deve considerar todos os aspectos dos processos de arquivamento, desde a criação e captura dos dados até a preservação e eliminação dos arquivos.
- Ao realizar a análise de riscos, a Autoridade Arquivística deve considerar os seguintes fatores:
- Ameaças: As ameaças podem ser internas ou externas. As ameaças internas podem incluir erros humanos, sabotagem e roubo de dados. As ameaças externas podem incluir ataques cibernéticos, desastres naturais e falhas de energia.
- Vulnerabilidades: As vulnerabilidades são fraquezas nos sistemas ou processos que podem ser exploradas pelas ameaças. As vulnerabilidades podem ser técnicas ou não técnicas. As vulnerabilidades técnicas podem incluir erros de software, configurações incorretas e hardware vulnerável. As vulnerabilidades não técnicas podem incluir falta de capacitação do pessoal, procedimentos de segurança inadequados e controles de usuários.

**COMPLEMENTO**

Você pode consultar o site da Agência Nacional de Segurança dos Sistemas de Informação do governo francês, para entender a aplicação de políticas de segurança, disponível no seguinte link: https:// cyber.gouv.fr/ , além disso, você pode consultar o Esquema Nacional de Segurança, desenvolvido pelo Governo da Espanha e disponível no seguinte link: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html

## 5.1. Funções de confiança

Quanto às responsabilidades do nível operacional, devemos distinguir pelo menos os seguintes papéis funcionais de confiança:

1. Gerente de segurança:

- Responsável por implementar e assegurar a aplicação da política de segurança.
- Gerencia os controles de acesso físico aos equipamentos.
- Autorizado para conhecer os arquivos relacionados com a atividade da Autoridade de Arquivo.
- Analisa os registros de eventos para detectar incidências, anomalias e tentativas de comprometimento.

2. Administrador da aplicação:

- Responsável por implementar a política de arquivo no nível da aplicação sob sua responsabilidade.
- Supervisiona todas as funções e o desempenho da aplicação.

3. Engenheiro de sistemas:

- Responsável pela implementação, configuração e manutenção técnica dos equipamentos de informática.
- Assegura a administração técnica de sistemas e redes

4. Administrador funcional:

- Gerencia os perfis de usuários para uma aplicação determinada.

5. Administrador de base de dados:

- Administra as bases de dados nas quais se baseiam as aplicações, com especial atenção aos direitos de acesso.

6. Agente de serviço de arquivo eletrônico:

- Opera as aplicações dentro do âmbito de suas atribuições.

Combinações de cargos proibidas:

- Gerente de segurança e engenheiro de sistemas
- Operador avaliador e qualquer outro cargo
- Engenheiro de sistemas e operador

## 5.2. Identificação, autenticação, integridade

### Controle de acesso e autenticação de usuários

Uma vez que um usuário tenha sido identificado e autenticado, é fundamental estabelecer um sistema de controle de acesso que limite seu acesso aos recursos e dados com base em seus direitos e permissões. Este sistema deve ser baseado em um diretório centralizado que armazene informações atualizadas sobre todos os usuários e seus respectivos direitos. O diretório deve ser atualizado periodicamente para refletir qualquer mudança nas permissões ou funções dos usuários.

Para garantir a segurança e a confiabilidade do acesso aos sistemas de arquivo, é essencial implementar mecanismos de autenticação robustos que permitam verificar com precisão a identidade dos usuários. Embora uma senha simples possa ser suficiente para consultas básicas no sistema, para acessos mais sensíveis, como os relacionados à administração, devem ser empregados métodos de autenticação mais robustos, como o uso de certificados eletrônicos.

### Controle de acesso a arquivos confidenciais

No caso de arquivos confidenciais, o controle de acesso deve ser gerenciado exclusivamente pelo serviço de arquivo eletrônico, restringindo o acesso apenas às pessoas autorizadas. O serviço de arquivo deve implementar mecanismos que permitam auditar e rastrear o acesso a esses arquivos sensíveis.

#### Verificação da integridade dos arquivos custodiados

A verificação da integridade dos arquivos custodiados deve ser realizada em múltiplas etapas do processo de arquivamento:

- Nível de transferência: O serviço de arquivos deve verificar a integridade dos arquivos durante a transferência inicial para garantir que não tenham sido alterados durante o processo de transmissão.
- Ciclo de vida do arquivo: A verificação da integridade deve ser possível a qualquer momento durante o ciclo de vida do arquivo, independentemente de possíveis migrações ou consultas por parte dos usuários. Para arquivos físicos, podem ser realizadas verificações periódicas por amostragem através da impressão dos documentos e comparação com cópias de referência.

#### Implementação de sistemas de verificação de integridade

A seleção e aplicação de sistemas de verificação de integridade devem considerar os seguintes aspectos:

- Tipo de arquivo: Os métodos de verificação devem se adaptar ao tipo de arquivo (físico, digital, etc.) e às características específicas do formato.
- Nível de risco: O nível de risco associado ao arquivo deve determinar a frequência e o rigor das verificações de integridade.
- Recursos disponíveis: A implementação de sistemas de verificação deve considerar os recursos técnicos e humanos disponíveis.

## 5.3. Rastreabilidade

Para compor um conjunto de dados suficiente e coerente em termos de rastreabilidade, é necessário realizar e validar as seguintes operações antes de iniciar qualquer serviço de arquivo eletrônico:

1. Identificação dos eventos a registrar

O primeiro passo consiste em identificar os diferentes tipos de eventos que serão registrados no sistema de arquivo eletrônico. Isso inclui eventos relacionados à criação, modificação, exclusão, acesso e transferência de arquivos, assim como eventos relacionados à configuração e manutenção do sistema.

2. Definição de informação registrada

Para cada tipo de evento identificado, deve-se definir as informações que serão registradas. Essas informações devem ser suficientes para permitir a rastreabilidade completa das ações realizadas dentro do sistema.

3. Notificações de eventos

Deve-se determinar se o administrador de eventos deve ser notificado sobre a gravação de um evento, e em que termos. Isso dependerá do tipo de evento e do seu potencial impacto na segurança ou no funcionamento do sistema.

4. Frequência de processamento dos registros

Deve-se definir uma frequência mínima para o processamento dos registros de eventos. Isso garantirá que os registros sejam processados de maneira oportuna e que a informação esteja disponível para sua análise em caso de necessidade.

5. Retenção de registros

Deve-se estabelecer um período de retenção para os registros de eventos. Esse período deve ser suficientemente longo para permitir a investigação de incidentes de segurança ou problemas de funcionamento, mas não deve ser excessivo para evitar o acúmulo de dados desnecessários.

6. Segurança dos registros

Devem ser verificados os dispositivos de segurança implementados para proteger os registros de eventos. Isso inclui medidas de controle de acesso, proteção contra intrusões e cópias de segurança.

7. Procedimento de armazenamento de registros

Deve-se consultar o procedimento estabelecido para o armazenamento dos registros de eventos. Isso garantirá que os registros sejam armazenados de maneira segura e que estejam acessíveis para consulta e análise.

8. Carimbo de tempo

Com o objetivo de garantir a integridade do carimbo de data/hora realizado pelo serviço, este se baseará em um processo de acordo com o estado da técnica. Atualmente, o RFC 3161 fornece uma referência para a implementação de carimbos de tempo confiáveis. Além disso, recomenda-se utilizar pelo menos duas fontes de tempo separadas para registrar as diferentes operações realizadas. Isso ajudará a prevenir a manipulação do carimbo de data/hora e a garantir a confiabilidade dos registros de eventos.

### 5.4. Plano de continuidade de negócios

Cada componente da Autoridade de Arquivo deve ter um plano de continuidade de negócios para cumprir com os requisitos de disponibilidade das diversas funções do processo de arquivo, o qual deve ser testado pelo menos uma vez ao ano.

Portanto, cada entidade que opera um componente da Autoridade de Arquivos deve implementar procedimentos e meios para informar e gerenciar incidentes, em particular por meio da conscientização e capacitação de seu pessoal e mediante a análise dos diversos registros de eventos.

## Capítulo 6. Conclusão

A incorporação da abordagem de sustentabilidade no âmbito arquivístico não se limita à mera implementação de um novo sistema, mas exige uma profunda reestruturação e reorientação da organização sob uma perspectiva holística. Essa abordagem implica uma transformação multifacetada que abrange diversos aspectos, desde os orçamentários e organizacionais até os profissionais, técnicos e culturais.

Embora não se trate de uma revolução radical, mas de uma evolução gradual, o processo de adoção da sustentabilidade pode apresentar desafios consideráveis, especialmente dependendo do grau de maturidade da organização. No entanto, é importante destacar que não se parte do zero, pois existem práticas e metodologias reconhecidas que podem ser adaptadas ao contexto arquivístico. Os fundamentos do arquivo, a gestão de riscos e as boas práticas de TI, por exemplo, podem ser perfeitamente integrados à abordagem de sustentabilidade.

A existência de normas e guias sobre o tema também contribui para oferecer maior clareza e segurança às organizações em seu processo de transição. No entanto, é crucial reconhecer que, para alcançar uma verdadeira transformação rumo à sustentabilidade, é necessário que tanto os arquivistas quanto os profissionais de TI adquiram novas habilidades e competências Embora os planos de formação sejam essenciais, é necessário ir além e repensar os programas educativos para preparar as novas gerações de profissionais a enfrentar os desafios da sustentabilidade no âmbito arquivístico.

Em definitivo, a incorporação da abordagem de sustentabilidade na organização arquivística requer um compromisso profundo e contínuo por parte de todos os atores envolvidos. Embora o caminho possa ser desafiador, os benefícios a longo prazo são significativos, tanto para a própria organização quanto para o meio ambiente e a sociedade como um todo.

# Bibliografia

Asociación Española de Normalización y Certificación. (2015). *Norma UNE-ISO 14721:2015 Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS) Modelo de referencia.* España: AENOR

BANAT-BERGER F., HUC C., DUPLOUY L., *L'Archivage numérique à long terme, les débuts de la maturité?* (Primera obra de síntesis sobre el archivo digital en lengua francesa) Paris, La Documentation française, 2009

BANAT-BERGER F., HUC C., Module 7 - Gestion et archivage des documents numériques. Portail International Archivistique Francophone. 2011. https://www.piaf-archives.org/se-former/module-7-gestion-et-archivage-des-documents-numeriques (Se identifica en el texto como PIAF)

Digital Information LifeCycle Interoperability Standards Board (DILCIS Board). (14 de 04 de 2024). Digital Information LifeCycle Interoperability Standards Board (DILCIS Board). Obtenido de eArchiving Standards & Specifications: https://dilcis.eu/

DLM FORUM. (14 de 04 de 2024). MoReq: modular requirements for records systems. Obtenido de MoReq2010: https://moreq.info/

Gobierno de España. (14 de 04 de 2024). Política de gestión de documentos electrónicos. Obtenido de Portal administración electrónica: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Politica-de-gestion-de-documentos-electronicos.html

Red de transparencia y acceso a la información. (14 de 04 de 2024). Modelo de Gestión de Documentos y Administración de Archivos (MGD) para la Red de Transparencia y Acceso a la Información (RTA). Obtenido de Guía de Implementación Gerencial– Política de gestión de documentos y archivos: http://mgd.redrta.org/guia-de-implementacion-gerencial-politica-de-gestion-de-documentos-y-archivos/mgd/2015-01-21/124946.html


IBERARCHIVOS
IBERARQUIVOS


ARCHIVO NACIONAL
COSTA RICA


UNIVERSIDAD DE
COSTA RICA