TRANSFORMAÇÃO DIGITAL

2025

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Gestão
e Recursos Humanos

Sumário

.

1.0 - EMENTA DO CURSO

Em 2025, a transformação digital na gestão e preservação de documentos digitais alcançou um patamar de maturidade, impulsionada pela necessidade de eficiência, transparência e segurança da informação. Diante desse cenário, todos os profissionais devem ficar atentos e se prontificar a serem protagonistas e fazer parte dessa mudança, adaptando suas práticas e conhecimentos para garantir a integridade e acessibilidade do patrimônio documental em um ambiente cada vez mais digital. O arquivista em especial, tem um papel fundamental nessa transformação, seja atuando no setor público ou privado. Surge um campo fértil para consultorias especializadas.

No setor público, a transformação digital tem sido crucial para a modernização dos serviços, a otimização dos processos e o aumento da transparência. A gestão eletrônica de documentos (GED) permite o acesso rápido e seguro às informações, agilizando a tomada de decisões e facilitando a comunicação com os cidadãos. A preservação digital garante a memória institucional e a prestação de contas, protegendo os documentos de valor histórico e probatório.

No setor privado, a transformação digital tem impulsionado a competitividade e a inovação. A gestão eficiente de documentos digitais reduz custos, aumenta a produtividade e facilita a colaboração entre equipes. A preservação digital protege os ativos informacionais das empresas, garantindo a conformidade com as regulamentações e a proteção da propriedade intelectual.

A importância da transformação digital na gestão e preservação de documentos digitais reside na sua capacidade de garantir o acesso à informação, a transparência, a segurança da informação e jurídica e a eficiência operacional. Ao adotar tecnologias e práticas adequadas, o setor público e privado podem construir um futuro mais informado, seguro, responsável e eficiente, além de proporcionar segurança jurídica e transparência ativa.

2.0 - CONTEÚDO PROGRAMÁTICO

MÓDULO 1: Transformação Digital

- Conceitos
- Os modelos de negócios
- Trajetória da transformação digital
- Como transformar digitalmente na gestão de documentos
- Debate em sala de aula

MÓDULO 2: Compliance e Governança

- Conceitos
- Legislação
- Normas
- Resoluções
- Debate em sala de aula

MÓDULO 3: Modelos de Requisito

- Conceitos
- E-ARQ Brasil
- MoReq-Jus
- Debate em sala de aula

MÓDULO 4: Lei Geral de Proteção de Dados - LGPD

- Conceitos
- Gestão de Privacidade
- Segurança da Informação
- Governança
- Educação Digital
- Debate em sala de aula

MÓDULO 5: Preservação Digital Sistêmica - PDS

- Conceitos
- Os modelos de negócios
- Trajetória da transformação digital
- Como transformar digitalmente na gestão de documentos
- Debate em sala de aula

3.0 - OBJETIVOS DO CURSO

Contribuir com o conhecimento sobre transformação digital, observando os riscos do uso da Tecnologia, demonstrando a importância da educação e ética digital e a responsabilidade ao utilizar as tecnologias. Identificação de modelos de negócio. Inovação Sustentada x Inovação Disruptiva. A evolução da Digitização, Digitalização e Implementação de novos modelos de negócio (Transformação Digital). Aprimorar o entendimento sobre a gestão de documentos digitais e as estratégias para uma preservação de documentos digitais de forma sistêmica. Capacitar o servidor público quanto a importância da proteção no ambiente digital entendendo a importância dos documentos digitais. O foco principal dessa capacitação é o aumento de maturidade do servidor público quanto ao uso das tecnologias e para uma transformação digital de forma responsável, ética e transparente.

4.0 - TRANSFORMAÇÃO DIGITAL

A transformação digital é o uso da tecnologia para aumentar de forma significativa a performance e o alcance das empresas por meio da mudança como os negócios são feitos. Por meio de novos investimentos em tecnologias e modelos de negócios, espera-se melhorar o engajamento dos clientes digitais em todos os pontos de contato no ciclo de vida de sua experiência.

Elementos da Transformação Digital (TD):

- Transformação da Experiência do Cliente
- Transformação dos Processos Operacionais
- Transformação dos Modelos de Negócio

A Transformação da Experiência do Cliente está pautado em:

- Entender o Cliente
- Nova Forma de Engajamento com o Cliente
- Pontos de Contato

A Transformação dos Processos Operacionais está pautado em:

- Digitalização de Processos
- Capacitação do Colaborador
- Gerenciamento de Performance

A Transformação dos Modelos de Negócio está pautado em:

- Modelos de Negócios Digitais
- Novos Negócios Digitais
- Globalização Digital

Os benefícios da Transformação Digital (TD)

- Agilidade em todas as etapas.
- Economia de recursos e tempo.
- Precisão na organização e validação de dados.
- Transparência com rastreabilidade total.

A Transformação Digital (TD) dentro do Estado, é mais um passo no avanço da gestão pública, simplificando processos e garantindo eficiência para servidores e gestores e transparência cada vez mais ativa.

MODELOS DE NEGÓCIO

A transformação digital (TD) nas instituições acontece a partir de demandas da sociedade (do nosso público-alvo, do mercado etc.), e de mudanças culturais, operacionais, pautadas nas necessidades e objetivos do negócio que oferecemos. Assim, o pontapé inicial consiste em uma avaliação do cenário atual dos nossos produtos ou serviços e de nossas estratégias e a definição de um Plano de TD ou Prospecção de TD.

A Transformação Digital (TD) é um conceito que surgiu no início dos anos 2000, com a popularização da Internet, dos computadores pessoais e do conceito de globalização dos anos 90. Desde então, a presença da tecnologia no cotidiano das instituições mais diversas tem sido cada vez maior e mais dinâmica, atendendo demandas e contexto.

Vejam que, impulsionada pelas inovações tecnológicas, a Transformação Digital é uma realidade para instituições de todos os setores. Além de fortalecer a presença digital de um negócio, marca ou setor, ela representa a implementação de soluções e automatizações nas mais diversas tarefas do dia a dia da instituição.

É uma mudança, uma guinada, com novos Modelos de Negócio, com Inovação, Conectividade, Usuários/Clientes e Dados, não é só digitizar nem digitalizar (estes são

passos para uma TD), então, vamos às pesquisas para os Arquivos: Mahraz; Benabbou; Berrado (2019, p. 922), destacam que o termo é relativamente antigo e que apareceu pela primeira vez em 2000 (Patel & McCarthy, 2000), estando associado ao que chamamos de digitalização (ou digitização, mas vejam, são termos distintos), mas, que agora, se refere a um fenômeno relacionado a novos usos dos consumidores (usuários) e objetos únicos que impactam diretamente nos atuais modelos de negócio e nas organizações, ou seja, o modelo negócio na TD se transforma continuamente.

Henriette et al. (2015), afirma que a TD é um processo de mudança disruptiva ou incremental (inovação sustentada, grifo nosso). Ele inicia com a adoção e uso de tecnologias digitais. Então, evoluindo para uma conversão holística implícita de uma organização, ou então, de forma deliberada na busca da criação de valor.

Khan (2016), alerta que existe uma confusão de conceitos entre digital, digitalização e transformação digital, no seu ponto de vista não existe uma determinação clara e amplamente aceita para se definir a transformação digital.

Roger (2017) diz que a transformação digital não tem a ver só com a tecnologia, e sim com estratégia e novas maneiras de pensar das organizações.

SOLIS; SZYMANSKI (2016, p. 4, Francisco, 2019) “A transformação digital é o realinhamento ou o investimento em novas tecnologias, modelos de negócio e processos para gerar valor para clientes funcionários e competir de forma mais eficaz em uma economia digital em constante mudança.”

KANE (2017, p. 2, Francisco, 2019) “A melhor compreensão da transformação digital é a adoção de processos e práticas empresariais para ajudar a organização a competir efetivamente em um Mundo cada vez mais digital.”

MÉNDEZ; ANDREU; TIRADOR (2015, p. 1) “A transformação digital é uma disciplina que afeta transversalmente as organizações, o seu modelo de Negócio e as suas competências. Realizar pequenos ajustes e alterações não é suficiente. Levar a cabo uma transformação digital significa dar aos utilizadores e aos clientes o nível de experiência que hoje exigem de todos os níveis da organização e, ao mesmo tempo, tornar a empresa mais competitiva face a novos atores e a novas ameaças. A

transformação digital é, em suma, o ponto de encontro entre as oportunidades tecnológicas e os novos modelos de negócio e crescimento. ”

Como surge o novo modelo de negócio ou preciso saber para criar?

1. Preciso atender as demandas da Sociedade de Transformar Digitalmente os Documentos, os Arquivos e a Formação do Arquivista?
2. Os Documentos Arquivísticos já foram Transformados Digitalmente, não? Alguns disruptivamente, outros por Inovação Sustentada…
3. E sobre os Arquivos, como transformá-los digitalmente?
4. Por quais motivos um Arquivo poderia ser transformado por Disrupção ou por Inovação Sustentada?
5. Os Arquivos estão elaborando seus Planos de Transformação Digital?
6. Quais elementos indicariam que um Arquivo é pró-Disruptivo ou pró-Inovação Sustentada? O seu Arquivo, ou da sua cidade, é?
7. Quais elementos de Transformação Digital e Alavancas-chave de valor o meu Arquivo possui?
8. E sobre a nossa formação como está, Transformada Digitalmente, ou para as demandas de TD?
9. E sobre a não adoção de Políticas do Software Livre em Arquivos, em Documentos Arquivísticos, Dados, públicos, que não poderiam ter nenhum tipo de restrição de acesso, uso, reuso, análises etc.?

TRAJETÓRIAS DA TRANSFORMAÇÃO DIGITAL (TD)

Há dois tipos básicos de inovação — **sustentada e disruptiva** — que seguem diferentes trajetórias e levam a diferentes resultados. Inovações sustentadas ajudam organizações líderes ou inovadoras a criarem melhores produtos ou serviços que frequentemente podem ser vendidos com maiores lucros a seus melhores clientes. Elas servem aos consumidores existentes de acordo com a definição original de desempenho — ou seja, de acordo com o modo como o mercado historicamente definiu o que é bom.

Um engano comum a respeito da teoria da inovação disruptiva é o de que as inovações disruptivas são **boas**, enquanto as inovações sustentadas são **ruins**. **Isto**

é falso. Precisamos de DIAGNÓSTICO! As inovações sustentadas são vitais para um setor saudável e robusto, na medida em que as organizações se esforçam para fazer melhores produtos e oferecer melhores serviços para seus melhores clientes.

As inovações disruptivas, por sua vez, não procuram trazer produtos melhores para clientes existentes em mercados estabelecidos. Em vez disso, elas oferecem uma nova definição do que é bom — assumindo normalmente a forma de produtos mais simples, mais convenientes e mais baratos que atraem clientes novos ou menos exigentes. Com o tempo, elas se aperfeiçoam o suficiente para que possam atender às necessidades de clientes mais exigentes, transformando um setor.

Devemos considerar, também, que a sociedade, e não somente o mercado, está demandando da Academia e dos profissionais "arquivistas", mudanças para que se crie, para que se adapte e se implemente modelos novos de negócio nos Arquivos.

Para o coletivo da cidadania, não importa se estas mudanças, transformações digitais, serão via trajetórias sustentadas ou disruptivas. E aí, exatamente neste ponto que vem a grande pergunta para nós: o que devemos considerar, quais referenciais nós temos de considerar para esse cenário de transformação digital?

O quão pró-Transformação Digital são ou estão os nossos Arquivos, ou pró-disruptivos, ou pró-inovação sustentada? Considerando que os Documentos já foram transformados digitalmente, e que toda esta mudança, também tem impacto na formação dos profissionais.

Exemplos de Tecnologias Disruptivas:

- UBER
- AIRBND
- NETFLIX
- WIKIPEDIA

Maturidade Digital dos Arquivos: "Mas, o que é "digital"?

Transformações digitais podem ser caracterizadas por acionar ao menos uma de quatro alavancas-chave de valor:

- **Modelos de negócio (**novas formas de operar e novos modelos econômicos);

- **Conectividade** (engajamento em tempo real);
- **Processos** (foco na experiência do cliente, automação e agilidade) e
- **Analytics** (melhor tomada de decisão e cultura de dados).

No entanto, para capturar o valor criado por essas alavancas, é necessário associá-las a um conjunto de melhores práticas de gestão que abrangem quatro dimensões fundamentais: **Estratégia**, **Capacidades**, **Organização** e **Cultura**.

Exemplos

- **Modelos de negócio** (Preservação Digital Sistêmica, oferecer custódia digital);
- **Conectividade** (Plataforma de Acesso e Transparência Ativa);
- **Processos** (Curadoria Digital Arquivística);
- **Analytics** (PCD, TTD e Instrumentos de Pesquisa em Dados).

O A&DQ mensura a maturidade digital de uma empresa em Analytics e digital em 4 dimensões e 22 práticas.

- **Estratégia**
- **Capacidade**
- **Organização**
- **Cultura**

ESTRATÉGIA

- Consciência da mudança: manifestada em algum documento;
- Aspiração ambiciosa e de longo prazo;
- Vinculado à estratégia de negócio: do Arquivo;
- Centralidade do Cliente: Plataformas de Acesso e Difusão;
- Oportunidades de crescimento;
- Roadmap específico: do Arquivo.

CAPACIDADES

- Marketing e vendas digitais: o CONSUMER do Modelo OAIS;
- Jornadas do cliente;
- Dados e Analytics, Documentos em DADOS ou COM Dados;
- Modelos e plataformas tecnológicas;
- Foco na geração de valor.

ORGANIZAÇÃO

- Estrutura, vinculação do Arquivo etc.;
- Colaboração entre negócio e tecnologia, o Arquivo e a TI;
- Talentos: quais competências dos Arquivistas e Técnicos;
- Proficiência em Analytics e Digital, nossos Arquivistas sabem trabalhar com dados, PCD em Dados, TTD em Dados etc.;
- Governança e métricas.

CULTURA

- Agilidade;
- Teste e aprendizado;
- Experimentação;
- Colaboração interna;
- Orientação externa;
- Mentalidade baseada em dados, Planta de engenharia, em dados, fotografias em dados etc.
- Cultura de Transparência

Existe uma preocupação com os impactos da Transformação Digital na Ciência da Informação e daí podemos derivar que também nos Arquivos, na Administração Pública e na sociedade como um todo, afinal, seus impactos nem sempre são positivos.

A transformação digital tornou-se assim um tema inevitável com enorme importância na realidade de hoje e do futuro e que abrange também um processo de adaptação ao mundo digital.

A sociedade contemporânea é pressionada para responder a estas mudanças e necessidades devido a uma constante evolução e à existência de quantidades cada vez maiores de dados.

É por isso necessário conhecer estas tendências e quais as competências necessárias e indispensáveis aos profissionais da informação para exercerem funções de gestão e curadoria.

5.0 - COMPLIANCE & GOVERNANÇA

Compliance: é um conjunto de regras e procedimentos que visa garantir que uma organização esteja em conformidade com as leis e regulamentos vigentes.

Governança: é conjunto de práticas e princípios que visam a tomada de decisões e a gestão de relações com a sociedade. Ela envolve a liderança, a estratégia e o controle de uma organização ou instituição.

Gestores públicos, preparem-se para uma jornada rumo à excelência na gestão! O compliance é mais do que um conjunto de regras, é um farol que guia nossas ações, garantindo a transparência, a ética e a legalidade em todas as nossas decisões.

Imagine uma empresa que navega em um mar tempestuoso sem bússola. Os riscos são imensos, não é mesmo? O compliance é essa bússola que nos orienta, evitando que naufragamos em um mar de irregularidades.

Ao adotar práticas de compliance, estamos:

- **Prevenindo riscos:** Identificando e mitigando possíveis irregularidades, como fraudes, corrupção e desvios de conduta.
- **Protegendo a reputação:** Demonstrando que a gestão pública é séria e transparente, aumentando a confiança da sociedade.
- **Assegurando a continuidade dos negócios:** Evitando multas, sanções e processos judiciais que podem paralisar as atividades da organização.
- **Otimizando recursos:** Utilizando os recursos públicos de forma eficiente e eficaz, em benefício da população.
- **Fortalecendo a cultura organizacional:** Criando um ambiente de trabalho baseado na ética, na integridade e no respeito às leis.

A implementação do compliance exige um esforço conjunto de todos os níveis da organização. Algumas dicas práticas incluem:

- Compromisso da Alta Administração
- Código de Conduta
- Treinamento e Comunicação
- Canais de Denúncia

- Avaliação de Riscos
- Controles Internos
- Due Diligence
- Monitoramento e Auditoria
- Investigação de Irregularidades
- Melhoria Contínua

Gestores públicos, a governança não é apenas uma tendência, mas uma necessidade imperativa para garantir a gestão eficiente e transparente dos recursos públicos. Ao adotar práticas de governança, vocês fortalecerão a confiança da sociedade e contribuindo para o desenvolvimento sustentável do Estado.

A Governança é um instrumento fundamental para modernizar a gestão pública e garantir a prestação de serviços de qualidade à sociedade. Ao adotar práticas de governança, os gestores públicos contribuirão para um futuro mais justo e transparente para todos.

É importante para:

- Transparência e Accountability
- Melhora na Tomada de Decisão
- Redução de Riscos
- Aumento da Eficiência
- Fortalecimento da Reputação

Benefícios da Governança para a segurança jurídica?

- **Prevenção de irregularidades:** Ao estabelecer mecanismos de controle e monitoramento, a governança reduz o risco de ocorrência de irregularidades, como fraudes e corrupção.
- **Conformidade com a legislação:** A governança garante o cumprimento das leis e regulamentos, evitando processos judiciais e sanções administrativas.
- **Proteção do patrimônio público:** Ao garantir a gestão adequada dos recursos públicos, a governança protege o patrimônio público de perdas e danos.

Implementação da Governança

- **Defina claramente os papéis e responsabilidades:** Estabeleça um sistema claro de atribuição de responsabilidades, definindo as funções de cada órgão e gestor.
- **Crie um código de conduta:** Elabore um código de conduta que estabeleça os princípios e valores que devem guiar a atuação dos servidores públicos.
- **Implemente mecanismos de controle interno:** Crie mecanismos de controle interno para monitorar as operações e garantir a conformidade com as normas e procedimentos.
- **Promova a transparência:** Divulgue as informações de forma clara e objetiva, facilitando o acesso da sociedade às ações do governo.
- **Incentive a participação:** Crie canais de participação para que a sociedade possa acompanhar e contribuir para a gestão pública.

O Compliance e a Governança não são custos, mas um investimento no futuro da gestão pública. Ao adotar práticas de compliance, estamos construindo uma gestão mais eficiente, transparente e ética, em benefício de toda a sociedade.

O Compliance e a Governança são processos contínuos que exige o comprometimento de todos os envolvidos.

Ao investir em Compliance e a Governança, investirá no futuro do seu município, estado ou país.

Ao transformar o Compliance e a Governança em uma cultura organizacional, daremos um grande passo rumo à excelência na gestão pública.

Legislações:

- Constituição da República Federativa do Brasil de 1988;
- Lei nº 8.159, de 08 de janeiro de 1991;
- Lei nº 12.527, de 18 de novembro de 2011;
- Lei nº 12.965, de 23 de abril de 2014;
- Lei nº 13.709, de 14 de agosto de 2018;
- Lei nº 14.063, de 23 de setembro de 2020.

Constituição da República Federativa do Brasil de 1988

Direitos e Garantias Fundamentais

5º, X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

5º, LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Emenda Constitucional nº 115, de 10 de fevereiro de 2022

Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais

5º, LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Competências:

21, XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.

22, XXX - proteção e tratamento de dados pessoais.

Lei nº 8.159, de 08 de janeiro de 1991

Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

Lei nº 12.527, de 18 de novembro de 2011

Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11

de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

Lei nº 12.965, de 23 de abril de 2014

Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Lei nº 13.709, de 14 de agosto de 2018

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Lei nº 13.853, 8 de julho de 2019

Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

Lei nº 14.063, de 23 de setembro de 2020.

Esta Lei dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos, com o objetivo de proteger as informações pessoais e sensíveis dos cidadãos, com base nos incisos X e XII do caput do art. 5º da Constituição Federal e na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), bem como de atribuir eficiência e segurança aos serviços públicos prestados sobretudo em ambiente eletrônico.

Normas Internacionais:

- Norma ISO 30300:2016
- Norma ISO 15489-1:2018
- Norma ISO 31000:2018

- Norma ISO 16167:2020
- Norma ISO 27701:2020
- Norma ISO 27001:2022
- Norma ISO 27002:2022
- Norma ISO 27005:2023

Norma ISO 30300:2016

Informação e documentação — Sistema de gestão de documentos de arquivo — Fundamentos e vocabulário.

Esta Norma estabelece termos e definições aplicáveis às normas elaboradas pelo ISO/TC 46/SC 11 para SGDA. Além disso, estabelece os objetivos de usar um SGDA, fornece princípios para um SGDA, descreve uma abordagem de processos e específica papéis da alta administração.

Esta Norma é aplicável a qualquer tipo de organização que deseje:

a) estabelecer, implementar, manter e aperfeiçoar um SGDA como apoio às suas atividades;

b) assegurar-se de sua conformidade com sua política declarada de documentos de arquivo;

c) demonstrar a conformidade com esta Norma por meio da:

1) realização de uma autoavaliação e autodeclaração; ou

2) busca da confirmação de sua autodeclaração por um terceiro; ou

3) busca da certificação de seu SGDA por um terceiro.

Norma ISO 15489-1:2018

Informação e documentação — Gestão de documentos de arquivo Parte 1: Conceitos e princípios

Esta Parte da **ABNT NBR ISO 15489** estabelece os conceitos e princípios fundamentais para a produção, captura e gerenciamento de documentos. Ela está no cerne de uma série de normas internacionais e relatórios técnicos que fornecem mais

orientações e instruções sobre os conceitos, técnicas e práticas para a produção, captura e gerenciamento de documentos de arquivo.

Os documentos de arquivo são tanto prova de atividade de negócios quanto ativos de informação. Eles podem ser diferenciados de outros ativos de informação por sua função como prova na transação de negócios e pela sua confiança em metadados.

Os metadados dos documentos de arquivo são usados para indicar e preservar o contexto e aplicar regras apropriadas para a gestão de documentos de arquivo.

A gestão de documentos de arquivo abrange o seguinte:

a) produção e captura de documentos de arquivo para cumprir os requisitos de prova da atividade de negócio;

b) adoção de medidas apropriadas para proteger sua confiabilidade, integridade e usabilidade conforme seu contexto de negócios e requisitos para gestão de mudanças ao longo do tempo.

Norma ISO 31000:2018

Gestão de riscos — Diretrizes

Este documento fornece diretrizes para gerenciar riscos enfrentados pelas organizações. A aplicação destas diretrizes pode ser personalizada para qualquer organização e seu contexto.

Este documento fornece uma abordagem comum para gerenciar qualquer tipo de risco e não é específico para qualquer indústria ou setor.

Este documento pode ser usado ao longo da vida da organização e aplicado a qualquer atividade, incluindo a tomada de decisão em todos os níveis.

Norma ISO 16167:2020

Segurança da informação — Diretrizes para classificação, rotulação, tratamento e gestão da informação

Esta Norma estabelece as diretrizes para classificação, rotulação, tratamento e gestão da informação, de acordo com a sua sensibilidade e criticidade para a organização, visando o estabelecimento de níveis adequados de proteção.

Norma ISO 27001:2022;

Segurança da informação — Diretrizes para classificação, rotulação, tratamento e gestão da informação

Esta Norma estabelece as diretrizes para classificação, rotulação, tratamento e gestão da informação, de acordo com a sua sensibilidade e criticidade para a organização, visando o estabelecimento de níveis adequados de proteção.

Norma ISO 27002:2022

Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação

Este documento é projetado para organizações de todos os tipos e tamanhos. É para ser usado como referência para determinar e implementar controles para tratamento de riscos de segurança da informação em um sistema de gestão de segurança da informação (SGSI) baseado na ABNT NBR ISO/IEC 27001. Também pode ser usado como um documento de orientação para organizações determinando e implementando controles de segurança da informação comumente aceitos. Além disso, este documento é destinado a ser utilizado no desenvolvimento de diretrizes de gestão de segurança da informação específicas para a indústria e a organização, considerando seu ambiente específico de riscos de segurança da informação. Controles organizacionais ou específicos do ambiente que não sejam os incluídos neste documento podem ser determinados através do processo de avaliação de riscos, conforme necessário.

Norma ISO 27701:2020;

Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes

Este documento especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização.

Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação.

Este documento fornece orientações para ajudar as organizações a:

- cumprir os requisitos da ABNT NBR ISO/IEC 27001 em relação às ações para abordar riscos de segurança da informação;
- realizar atividades de gestão de riscos de segurança da informação, especificamente avaliação e tratamento de riscos de segurança da informação.

Este documento é aplicável a todas as organizações, independentemente do tipo, tamanho ou setor.

Norma ISO 27005:2023

Este documento especifica os requisitos relacionados ao SGPI e fornece as diretrizes para os controladores de DP e operadores de DP que têm responsabilidade e responsabilização com o tratamento de DP (Dados Pessoais).

Este documento é aplicável a todos os tipos e tamanhos de organizações, incluindo as companhias públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que são controladoras de DP e/ou que são operadoras de DP.

Resoluções do CONARQ - Conselho Nacional de Arquivos

- Resolução nº 37, de 19 de dezembro de 2012.
- Resolução nº 38, de 9 de julho de 2013;
- Resolução nº 40, de 9 de dezembro de 2014 (alterada);
- Resolução nº 41, de 9 de dezembro de 2014;

- Resolução nº 42, de 9 de dezembro de 2014;
- Resolução nº 47, de 26 de abril de 2021;
- Resolução nº 48, de 10 de novembro de 2021;
- Resolução nº 50, de 06 de maio de 2022;
- Resolução nº 51, de 25 de agosto de 2023;
- Resolução nº 54, de 8 de dezembro de 2023;

Resolução nº 37, de 19 de dezembro de 2012

As Diretrizes de que trata essa resolução têm por finalidade instrumentalizar os produtores e custodiadores de documentos arquivísticos para essa presunção da autenticidade desses documentos.

A autenticidade dos documentos arquivísticos digitais deve estar apoiada em procedimentos de gestão arquivística de documentos.

Resolução nº 38, de 9 de julho de 2013

Recomendar aos órgãos e entidades integrantes do Sistema Nacional de Arquivos - **SINAR**, a adoção das Diretrizes do Produtor - A Elaboração e a Manutenção de Materiais Digitais: Diretrizes Para Indivíduos e Diretrizes do Preservador - A Preservação de Documentos Arquivísticos digitais: Diretrizes para Organizações, publicadas no âmbito do Projeto The International Research on Permanent Authentic Records in Electronic Systems **InterPARES**, da Universidade de British Columbia, Canadá, em acordo técnico com o Arquivo Nacional, visando ao aperfeiçoamento da gestão e preservação dos documentos de arquivo em formato digital.

Resolução nº 40, de 9 de dezembro de 2014 (alterada)

A eliminação de documentos digitais e não digitais no âmbito dos órgãos e entidades integrantes do SINAR ocorrerá depois de concluído o processo de avaliação e seleção conduzido pelas respectivas Comissões Permanentes de Avaliação de Documentos - CPAD e será efetivada quando cumpridos os procedimentos estabelecidos nesta Resolução.” (Redação dada pela Resolução nº 44, de 14 de fevereiro de 2020).

Resolução nº 41, de 9 de dezembro de 2014

Implementar política de gestão arquivística de documentos integrando todos os gêneros documentais, incluindo os audiovisuais, iconográficos, sonoros e musicais, independentemente do formato e do suporte em que estão registrados, por meio da classificação e avaliação arquivística, bem como dos procedimentos e operações técnicas referentes à produção, tramitação e uso;

Aplicar e padronizar a descrição arquivística, com base na Norma Brasileira de Descrição Arquivística - NOBRADE, aprovada pela Resolução nº 28, de 17 de fevereiro de 2009, do CONARQ, visando o acesso às informações contidas nos documentos de arquivo e propiciando o intercâmbio de informações arquivísticas entre instituições detentoras de acervos audiovisuais, iconográficos, sonoros e musicais.

Resolução nº 42, de 9 de dezembro de 2014

Não recomendar a utilização de papéis reciclados fabricados apenas com fibras curtas, secundárias não selecionadas, que contenham corantes e lignina para a produção de documentos arquivísticos, conforme as amostras analisadas no documento anexo a esta resolução, por terem sido reprovados em testes realizados para verificar suas qualidades físico-químicas e por não estarem em conformidade com as normas ISO 9706 (1994) e ISO 11108 (1996).

Resolução nº 47, de 26 de abril de 2021

Esta resolução estabelece os procedimentos relativos à declaração de interesse público e social de arquivos privados de pessoas físicas ou jurídicas que contenham documentos relevantes para a história, a cultura e o desenvolvimento nacional.

Resolução nº 48, de 10 de novembro de 2021

Estabelecer diretrizes e orientações aos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR quanto aos procedimentos técnicos a serem observados no processo de digitalização de documentos públicos ou privados.

Resolução nº 50, de 06 de maio de 2022

Esta resolução estabelece o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, Versão 2.

O **e-ARQ Brasil** tem por objetivo orientar aos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR quanto à implantação da gestão arquivística de documentos, fornecer especificações técnicas e funcionais, bem como metadados para orientar a aquisição ou desenvolvimento de sistemas informatizados, independentemente da plataforma tecnológica em que forem desenvolvidos ou implantados, conforme art. 3º da Resolução nº 20, de 16 de julho de 2004.

Resolução nº 51, de 25 de agosto de 2023

Estabelecer a segunda versão das "Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis", aprovada pelo Conselho Nacional de Arquivos (Conarq) na 103ª reunião plenária ordinária, realizada em 31 de agosto de 2022.

Estas Diretrizes têm por objetivo orientar aos órgãos e entidades integrantes do Sistema Nacional de Arquivos (Sinar) quanto à indicação de parâmetros e requisitos para repositórios arquivísticos digitais confiáveis, de forma a garantir a autenticidade (identidade e integridade), a confidencialidade, a disponibilidade, o acesso e a preservação, tendo em vista a necessidade de manutenção dos acervos documentais por longos períodos ou, até mesmo, permanentemente.

Resolução nº 54, de 8 de dezembro de 2023

Esta resolução estabelece diretrizes e regras para o tratamento de dados pessoais em arquivos permanentes, independentemente do suporte, visando à garantia dos direitos fundamentais de acesso à informação, intimidade, proteção dos dados pessoais e acesso às fontes da cultura nacional.

Aplica-se esta resolução aos integrantes do Sistema Nacional de Arquivos (SINAR) e a pessoas físicas e jurídicas de direito público ou privado, detentoras de arquivos.

6.0 - MODELOS DE REQUISITOS

Os modelos de requisitos e-ARQ Brasil e MoReq-Jus representam marcos fundamentais na jornada da transformação digital, especialmente no contexto da gestão e preservação de documentos digitais. Eles oferecem um arcabouço sólido para a implementação de Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD) eficientes e confiáveis.

O e-ARQ Brasil, desenvolvido pelo Conselho Nacional de Arquivos (CONARQ), estabelece diretrizes para a gestão de documentos digitais em todo o território nacional. Já o MoReq-Jus, criado pelo Conselho Nacional de Justiça (CNJ), foca nas especificidades do Poder Judiciário, garantindo a interoperabilidade e a segurança dos documentos judiciais eletrônicos.

A adoção desses modelos é crucial para assegurar a autenticidade, a integridade, a acessibilidade e a preservação dos documentos digitais ao longo do tempo. Eles fornecem um conjunto de requisitos técnicos e funcionais que orientam o desenvolvimento e a implementação de SIGADs, garantindo a conformidade com as normas e regulamentações vigentes.

Ao seguir os modelos e-ARQ Brasil e MoReq-Jus, as organizações podem otimizar seus processos de gestão documental, reduzir custos, aumentar a eficiência e garantir a transparência e a segurança da informação. Além disso, a padronização proporcionada por esses modelos facilita a interoperabilidade entre sistemas e a troca de informações entre diferentes instituições.

e-ARQ Brasil

Temo como finalidade ser um Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Este modelo deve ser seguido para uma gestão de documentos mais assertiva, seja na esfera pública ou privada.

O que representa o e-ARQ Brasil?

É uma especificação de requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir sua confiabilidade e autenticidade, assim como seu acesso, pelo tempo que for necessário.

Além disso, o e-ARQ Brasil pode ser usado para orientar a identificação de documentos arquivísticos digitais.

Funcionalidades do e-ARQ Brasil

O e-ARQ Brasil estabelece requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), independentemente da plataforma tecnológica em que for desenvolvido e/ou implantado.

Os requisitos dirigem-se a todos que fazem uso de sistemas informatizados como parte do seu trabalho rotineiro de produzir, receber, armazenar e acessar documentos arquivísticos. Um SIGAD pode incluir um sistema de protocolo informatizado, entre outras funções da gestão arquivística de documentos.

O e-ARQ Brasil especifica todas as atividades e operações técnicas da gestão arquivística de documentos. Todas essas atividades poderão ser desempenhadas pelo SIGAD, o qual, tendo sido desenvolvido em conformidade com os requisitos aqui apresentados, conferirá credibilidade à produção e à manutenção de documentos arquivísticos.

Motivação para criação do modelo

O e-ARQ Brasil considerou a existência de um importante acervo de documentos digitais que vem sendo tratado por especialistas de diversas áreas, entre as quais arquivologia e tecnologia da informação. O documento partiu da definição dos conceitos de documento arquivístico e documento arquivístico digital, tendo como base os fundamentos da diplomática e da arquivologia, enfatizando os conceitos e a prática de gestão de documentos, para fornecer um conjunto de requisitos que seja amplo, rigoroso e de qualidade.

Objetivos do e-ARQ Brasil

- Orientar a implantação da gestão arquivística de documentos arquivísticos digitais e não digitais;
- fornecer especificações técnicas e funcionais, além de metadados, para orientar a aquisição e/ou a especificação e desenvolvimento de sistemas informatizados de gestão arquivística de documentos.

Aplicação do Modelo

O e-ARQ Brasil deve ser utilizado para desenvolver um sistema informatizado ou para avaliar um já existente, cuja atividade principal seja a gestão arquivística de documentos.

O e-ARQ Brasil é aplicável aos sistemas que produzem e mantêm somente documentos digitais e aos sistemas que compreendem documentos digitais, não digitais e híbridos. Com relação aos documentos não digitais, o sistema apenas apoia o registro dos metadados desses documentos. No caso dos documentos digitais, o sistema inclui os próprios documentos, ou a referência a documentos digitais externos ao SIGAD, além dos metadados.

Desde que a organização estabeleça um programa de gestão arquivística de documentos, o e-ARQ Brasil é aplicável aos setores público e privado de qualquer esfera e âmbito de atuação, servindo para todos os tipos de documentos arquivísticos. Destina-se, igualmente, aos documentos relativos às atividades-meio e às atividades-fim de um órgão ou entidade e não se restringe a um ramo de atividade específica. Pode ser adotado como padrão ou norma pela administração pública federal, estadual, municipal, dos poderes Executivo, Legislativo e Judiciário, a fim de uniformizar o desenvolvimento e aquisição de sistemas que visem produzir e manter documentos arquivísticos em formato digital.

Para quem é recomendado?

- profissionais da gestão arquivística de documentos: para orientar a execução desses serviços a partir de uma abordagem arquivística;
- profissionais de tecnologia da informação: para orientar o desenvolvimento de um SIGAD em conformidade com os requisitos exigidos;
- auditores: como base para auditoria ou inspeção do SIGAD instalado;
- potenciais usuários de um SIGAD: como apoio na elaboração de edital para apresentação de propostas de fornecimento de software;
- potenciais compradores de serviços externos de gestão de documentos: como material auxiliar para a especificação dos serviços a serem comprados;

- instituições acadêmicas e organizações de formação profissional: como um documento de referência e recurso de ensino para a formação em gestão arquivística de documentos.

Estrutura do e-ARQ Brasil

O e-ARQ Brasil está dividido em duas partes. A Parte I, Gestão arquivística de documentos, pretende fornecer um arcabouço teórico e conceitual para que cada órgão ou entidade possa desenvolver um programa de gestão arquivística de documentos. A Parte II, Especificação de requisitos para sistemas informatizados de gestão arquivística de documentos, descreve os requisitos necessários para desenvolver o SIGAD.

A Parte I contém nove capítulos, alguns divididos em seções, e trata da política arquivística, do planejamento e da implantação do programa de gestão arquivística de documentos, dos procedimentos e controles do SIGAD e dos instrumentos utilizados na gestão de documentos.

A Parte II está organizada em requisitos funcionais, requisitos não funcionais, metadados, glossário e referências.

Requisitos Funcionais do e-ARQ Brasil

São aqueles que especificam uma função que o sistema deve ser capaz de realizar sob o ponto de vista do usuário final. Os requisitos funcionais tratam de organização de documentos (incluindo o plano de classificação), captura, avaliação (incluindo a destinação), recuperação da informação, elaboração de documentos, tramitação, segurança e preservação.

Requisitos não Funcionais do e-ARQ Brasil

São aqueles que não estão diretamente relacionados à funcionalidade do sistema, mas que são relevantes para a sua implementação.

Dessa forma, ressalta-se que, quando da implantação de um SIGAD, é necessário verificar e observar o cumprimento desses requisitos, considerando os contextos

jurídico, administrativo e tecnológico de cada instituição de maneira a cumprir com os requisitos desta especificação.

Os requisitos não funcionais tratam de armazenamento, funções administrativas, conformidade com a legislação e regulamentações, usabilidade, interoperabilidade, disponibilidade, desempenho e escalabilidade.

Transformação Digital na Gestão de Documentos

O avanço das tecnologias de informação e comunicação (TIC), a partir dos anos 1990, muda radicalmente os mecanismos de registro e comunicação da informação nas instituições públicas e privadas. Os documentos produzidos no decorrer das atividades dessas instituições, até então em meio não digital, assumem novas características, isto é, passam a ser gerados em ambientes eletrônicos, armazenados em suportes magnéticos e ópticos, em formato digital, e deixam de ser apenas entidades físicas para se tornarem entidades lógicas. Além disso, o gerenciamento dos documentos, tanto os digitais como os não digitais, começa a ser feito por meio de um sistema informatizado conhecido como gerenciamento eletrônico de documentos (GED).

Os documentos digitais trouxeram uma série de vantagens no que se refere à produção, transmissão, armazenamento e acesso que, por sua vez, acarretaram alguns problemas. A simplicidade de criação e transmissão de documentos traz como consequência a informalidade na linguagem, nos procedimentos administrativos, bem como o esvaziamento das posições hierárquicas. A facilidade de acesso acarreta, às vezes, intervenções não autorizadas que podem resultar na adulteração ou perda dos documentos. A rápida obsolescência tecnológica (software, hardware e formatos) e a degradação das mídias digitais dificultam a preservação de longo prazo dos documentos e seu acesso contínuo. Estes e outros problemas requerem a adoção de medidas preventivas para minimizá-los.

Conceitos importantes para Transformação Digital

O que é documento?
É uma unidade de registro de informações, qualquer que seja o formato ou o suporte.

O que é documento arquivístico?

É um documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência.

O que é documento digital?

É a informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional.

O que é documento arquivístico digital?

É um documento digital reconhecido e tratado como um documento arquivístico.

O que é o SIGAD?

É um sistema informatizado que apoia a gestão arquivística de documentos.

O sucesso do SIGAD dependerá, fundamentalmente, da implementação prévia de um programa de gestão arquivística de documentos.

O SIGAD deve ser capaz de gerenciar, simultaneamente, os documentos digitais, não digitais e híbridos.

No caso dos documentos não digitais, o sistema registra apenas as referências sobre os documentos.

O que é necessário para ser um SIGAD?

- captura, armazenamento, indexação e recuperação de todos os tipos de documentos arquivísticos;
- captura, armazenamento, indexação e recuperação de todos os componentes digitais do documento arquivístico como uma unidade complexa;
- gestão dos documentos a partir do plano de classificação para manter a relação orgânica entre os documentos;
- registro de metadados associados aos documentos para descrever os contextos desses mesmos documentos (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico);

- estabelecimento de relacionamento entre documentos digitais, não digitais e híbridos;
- manutenção da autenticidade dos documentos;
- aplicação de tabela de temporalidade e destinação de documentos, permitindo a seleção dos documentos para eliminação ou para guarda permanente;
- exportação de documentos para apoiar a transferência e o recolhimento;
- apoio à preservação dos documentos.

Atenção ao SIGAD

É preciso esclarecer que um **SIGAD** se diferencia de sistemas de Gerenciamento Eletrônico de Documentos (**GED**) e de Enterprise Content Management (**ECM**), que também realizam gerenciamento de documentos, mas não necessariamente com abordagem arquivística.

Gerenciamento Eletrônico de Documentos (GED)

Conjunto de tecnologias utilizadas para organização da informação não estruturada de um órgão ou entidade, que pode ser dividido nas seguintes funcionalidades: captura, gerenciamento, armazenamento e distribuição.

Entende-se por informação não estruturada aquela que não está armazenada em banco de dados, como mensagens de correio eletrônico, arquivo de texto, imagem ou som, planilhas etc.

O GED pode englobar tecnologias de digitalização, automação de fluxos de trabalho (workflow), processamento de formulários, indexação, gestão de documentos, repositórios, entre outras.

Enterprise Content Management (ECM)

Termo amplo para tecnologia digital, estratégias e métodos utilizados para capturar, gerir, acessar, integrar, medir e armazenar informação. Pode incluir módulos específicos para documentos que apoiam as atividades das organizações e ajudam no processo de tomada de decisão.

Considerações dos Sistemas:

Um GED ou um ECM tratam os documentos de maneira compartimentada, enquanto o SIGAD parte de uma concepção orgânica, qual seja, a de que os documentos possuem uma interrelação que reflete as atividades da instituição que os criou. Além disso, diferentemente do SIGAD, o GED ou o ECM nem sempre incorporam o conceito arquivístico de ciclo de vida dos documentos.

O papel do SINAR

O Sistema Nacional de Arquivos (SINAR) tem o CONARQ como órgão central e é composto pelo Arquivo Nacional, pelos arquivos dos poderes Executivo, Legislativo e Judiciário federais, e pelos arquivos estaduais, do Distrito Federal e municipais. Podem ainda integrar o SINAR as pessoas físicas e jurídicas de direito privado, detentoras de arquivos, mediante acordo com o CONARQ.

O SINAR tem por finalidade implementar a política nacional de arquivos públicos e privados, em conformidade com as diretrizes e normas emanadas pelo CONARQ, promovendo a gestão, a preservação e o acesso às informações e aos documentos na esfera de competência dos integrantes do SINAR.

Implantação do programa de gestão arquivística de documentos

A implantação do programa de gestão arquivística de documentos envolve a execução e o acompanhamento de ações e projetos, efetuados simultaneamente. Deve atender aos objetivos definidos no planejamento do programa no que se refere à capacitação de pessoal, implantação de sistemas de gestão arquivística, integração com os sistemas de informação existentes e os processos administrativos do órgão ou entidade. Essa etapa pode incluir a suspensão de atividades e procedimentos vigentes que forem considerados inadequados.

A execução propriamente dita significa pôr em prática os planos de ação e os projetos aprovados.

O acompanhamento da implantação ocorre por meio de relatórios, sumários, gráficos, reuniões e entrevistas, entre outros. O acompanhamento percorre todo o processo de implantação e pode implicar revisão e correções operacionais e estratégicas.

A revisão deve gerar decisões, providências e medidas de aperfeiçoamento do próximo ciclo do planejamento da gestão arquivística de documentos.

Exigências a serem cumpridas pelo programa de gestão arquivística de documentos:

O programa de gestão arquivística de documentos terá que atender a uma série de exigências, tanto em relação ao documento arquivístico como ao seu próprio funcionamento.

O documento arquivístico deve:

- refletir corretamente o que foi comunicado, decidido ou a ação implementada;
- conter os metadados necessários para documentar a ação;
- ser capaz de apoiar as atividades;
- prestar contas das atividades realizadas.

O programa de gestão arquivística de documentos deve:

- contemplar o ciclo de vida dos documentos;
- garantir o acesso aos documentos;
- manter os documentos em ambiente seguro;
- reter os documentos somente pelo período estabelecido na tabela de temporalidade e destinação;
- implementar estratégias de preservação dos documentos desde a sua produção e pelo tempo que for necessário;
- garantir as seguintes características do documento arquivístico: relação orgânica, unicidade, confiabilidade, autenticidade e acessibilidade.

Procedimentos e operações técnicas do sistema de gestão arquivística de documentos digitais e não digitais:

CAPTURA: Registro; Classificação; Indexação; Atribuição de Restrição de Acesso e Arquivamento.

Registro

O registro tem por objetivo demonstrar que o documento foi produzido ou recebido pelo órgão ou entidade e capturado pelo sistema de gestão arquivística de documentos, assim como facilitar sua recuperação.

Classificação

É o ato ou efeito de analisar e identificar o conteúdo dos documentos arquivísticos e de selecionar a classe sob a qual serão recuperados. Essa classificação é feita a partir de um plano de classificação elaborado pelo órgão ou entidade e que pode incluir ou não a atribuição de código aos documentos.

Indexação

Indexação é a atribuição de termos à descrição do documento.

Atribuição de Restrição de Acesso

Os documentos que dizem respeito à segurança da sociedade e do Estado, a sigilo comercial, bancário, industrial, telefônico, segredo de justiça, dentre outros, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas estarão sujeitos a restrições de acesso, conforme legislação em vigor.

Arquivamento

Arquivar é a técnica de colocar e conservar numa mesma ordem, devidamente classificados de acordo com o plano de classificação, todos os documentos de um órgão ou entidade, utilizando métodos adequados, de forma que fiquem protegidos e sejam facilmente localizados e manuseados.

AVALIAÇÃO

É o processo de análise dos documentos arquivísticos, visando estabelecer os prazos de guarda e a destinação, de acordo com os valores primário e secundário que lhes são atribuídos.

Os prazos de guarda e as ações de destinação deverão estar formalizados na tabela de temporalidade e destinação do órgão ou entidade.

TEMPORALIDADE

O sistema de gestão arquivística de documentos, particularmente no caso de um SIGAD, deve identificar a temporalidade e a destinação previstas para o documento no momento da captura e do registro, de acordo com os prazos e ações estabelecidos na tabela de temporalidade e destinação do órgão ou entidade. Essa informação deve ser registrada em um metadado associado ao documento.

O sistema de gestão arquivística de documentos também deve poder identificar os documentos que já cumpriram sua temporalidade, para implementar a destinação prevista. Se for um sistema de gestão arquivística de documentos (SIGAD), esse sistema deve ser capaz de listar os documentos que tenham cumprido o prazo previsto na tabela de temporalidade e destinação.

DESTINAÇÃO

As determinações sobre a destinação devem ser aplicadas aos documentos, de forma sistemática, no curso das atividades rotineiras do órgão ou entidade. Essas determinações não podem ser implementadas em documentos que estejam com pendências, sob litígio ou investigação.

ELIMINAÇÃO

Eliminar significa destruir os documentos que, na avaliação, foram considerados sem valor para guarda permanente.

A eliminação deve ser precedida da elaboração da listagem, do edital de ciência de eliminação e do termo de eliminação, de acordo com a legislação vigente, e deve obedecer a princípios e critérios.

TRANSFERÊNCIA

É a passagem de documentos do arquivo corrente para o arquivo intermediário, onde aguardarão o cumprimento dos prazos de guarda e a destinação final. Ao serem transferidos, os documentos devem ser acompanhados de listagem de transferência.

RECOLHIMENTO

É a entrada de documentos em arquivos permanentes de acordo com a jurisdição arquivística a que pertencem.

Os documentos a serem recolhidos devem ser acompanhados de instrumentos que permitam sua identificação e controle, segundo a legislação vigente.

Não deverão ser encaminhados ao recolhimento documentos com classificação em grau de sigilo e/ou submetidos à criptografia, antes de sua desclassificação e/ou remoção da criptografia.

Os procedimentos de transferência e recolhimento de documentos digitais para instituição arquivística que impliquem a transposição desses documentos de um SIGAD para outro sistema informatizado deve adotar providências e boas práticas no que diz respeito a:

- compatibilidade de suporte e formato, de acordo com as normas previstas pela instituição arquivística recebedora;
- documentação técnica necessária para interpretar o documento digital (processamento e estrutura dos dados);
- instrumento descritivo que inclua os metadados atribuídos aos documentos digitais e informações que possibilitem a presunção de autenticidade dos documentos recolhidos à instituição arquivística;
- informações sobre as migrações realizadas no órgão produtor.

PESQUISA, LOCALIZAÇÃO E APRESENTAÇÃO DOS DOCUMENTOS

O sistema de gestão arquivística deve prever funções de recuperação e acesso aos documentos e às informações neles contidas, de forma a facilitar a condução das atividades e satisfazer os requisitos relativos à transparência do órgão ou entidade. A recuperação inclui pesquisa, localização e apresentação dos documentos.

SEGURANÇA: Controle de Acesso; Trilhas de Auditoria; Cópias de Segurança e Segurança de Infraestrutura.

Controle de Acesso

O sistema de gestão arquivística precisa limitar ou autorizar o acesso a documentos por usuário e/ou grupos de usuários.

Trilhas de Auditoria

Registra o movimento e o uso dos documentos arquivísticos dentro de um SIGAD (captura, registro, classificação, indexação, arquivamento, armazenamento, recuperação da informação, acesso e uso, preservação e destinação), informando quem operou, a data e a hora, e as ações realizadas. A trilha de auditoria tem o objetivo de fornecer informações sobre o cumprimento das políticas e regras da gestão arquivística de documentos do órgão ou entidade.

Cópias de Segurança

O SIGAD deve prever controles para proporcionar a salvaguarda regular dos documentos arquivísticos e dos seus metadados. Deve também poder recuperá-los rapidamente em caso de perda devido a sinistro, falhas no sistema, contingência, quebra de segurança ou degradação do suporte. Esses mecanismos devem seguir a política de segurança da informação do órgão ou entidade.

Segurança da Infraestrutura

A natureza das medidas de segurança da infraestrutura de instalações do acervo digital diz respeito a requisitos operacionais e não é muito diferente daquela do acervo não digital.

ARMAZENAMENTO

Armazenar é guardar os documentos arquivísticos em local apropriado. No caso dos documentos digitais, esse armazenamento se dá em dispositivos de memória não voláteis.

Documentos de valor permanente, independentemente do formato, requerem um armazenamento criterioso desde o momento da sua produção, para garantir sua preservação no longo prazo.

PRESERVAÇÃO

As estratégias de preservação de documentos arquivísticos devem ser selecionadas com base em sua capacidade de manter as características desses documentos e na avaliação custo-benefício.

Podem incluir monitoramento e controle ambiental, restrições de acesso, cuidados no manuseio

direto e obtenção de suportes e materiais mais duráveis (papel, tinta, disco óptico, fita magnética).

Considerações sobre o e-ARQ Brasil

É o modelo de requisitos aplicado na Administração Pública e no Setor Privado. Não é aplicado no Judiciário, tem modelo próprio.

Um grande aliado no processo de transformação digital no que diz respeito a gestão de documentos (digitais e não digitais, por meio de um planejamento arquivístico e apoiado por um SIGAD.

MODELO DE REQUISITOS MOREQ-JUS

Tem como finalidade ser um Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (**MoReq-Jus**).

Objetivo:

Foi instituído em razão da necessidade de se estabelecerem requisitos mínimos de Gestão Documental para os sistemas informatizados do Poder Judiciário, de forma a garantir a confiabilidade, a autenticidade e a acessibilidade dos documentos e processos geridos por referidos sistemas pelo prazo necessário ao atendimento da legislação.

Critérios do MOREQ-JUS:

Estabelece critérios a serem cumpridos na captura, na produção, na classificação, na tramitação, na guarda, na avaliação, na seleção, no armazenamento, na indexação, na preservação, no arquivamento e no recebimento, pelos sistemas de gestão de processos e documentos digitais, não digitais ou híbridos, a fim de garantir a sua confiabilidade, autenticidade e acesso.

O MoReq-Jus estabelece requisitos mínimos para um Sistema Informatizado de Gestão de Processos e Documentos (**GestãoDoc**), independentemente da plataforma tecnológica em que for desenvolvido e implantado.

GESTÃODOC (MOREQ-JUS):

Um **GestãoDoc** deve ser capaz de gerenciar documentos e processos digitais, não digitais e híbridos.

Para os documentos não digitais, o sistema registra as referências a esses documentos e as operações de produção, de tramitação, de guarda, de armazenamento, de preservação, de arquivamento e de recebimento, podendo conter versões digitais desses documentos físicos. No caso dos sistemas de documentos digitais, esses registram também os documentos e as operações mencionadas.

A gestão de documentos não é questão afeta apenas às unidades de Arquivo, de Gestão Documental ou às Comissões Permanentes de Avaliação Documental, pois visa a garantir a produção, a guarda e o acesso aos documentos durante todo o seu ciclo de vida. Portanto, envolve os diversos atores e unidades da instituição e precisa

também atender as demandas dos cidadãos, que são o destinatário dos serviços judiciais.

Sistema desenvolvido para produzir, gerenciar a tramitação, receber, armazenar, dar acesso e destinar documentos em ambiente eletrônico. Pode compreender um software particular, um determinado número de softwares integrados — adquiridos ou desenvolvidos — ou uma combinação desses. Envolve um conjunto de procedimentos e operações técnicas característicos do sistema de gestão de processos e documentos, processado eletronicamente e aplicável em ambientes digitais ou em ambientes híbridos — documentos digitais e não digitais ao mesmo tempo.

Um GestãoDoc inclui diversas operações, tais quais, produção do documento, controle de sua tramitação, aplicação do plano de classificação, controle de versões, controle sobre os prazos de guarda e destinação, armazenamento seguro e procedimentos que garantam o acesso e a preservação a médio e longo prazo de documentos digitais e não digitais, mantendo-os confiáveis, íntegros e autênticos.

O Modelo de Requisitos utilizado pela Administração Pública e pelo setor Privado é o e-ARQ Brasil e seu sistema é chamado de SIGAD.

O Modelo de Requisitos utilizado pelo Judiciário é o MoReq-Jus e seu sistema é chamado de GestãoDoc.

7.0 - LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Exceto:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais

Fundamentos da LGPD:

I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Tratamento de Dados pelo Poder Público

O tratamento de dados pessoais pelo Poder Público possui muitas peculiaridades, que decorrem, em geral, da necessidade de compatibilização entre o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na Lei Geral de Proteção de Dados Pessoais.

Oportunidades e Desafios

Diante desse cenário, o desafio posto é o de estabelecer parâmetros objetivos, capazes de conferir segurança jurídica às operações com dados pessoais realizadas por órgãos e entidades públicos. Trata-se de assegurar a celeridade e a eficiência necessárias à execução de políticas e à prestação de serviços públicos com respeito aos direitos à proteção de dados pessoais e à privacidade.

O que precisam fazer?

Órgãos e entidades públicos têm questionado a Autoridade Nacional de Proteção de Dados (ANPD) sobre:

- o âmbito de incidência da LGPD e a aplicação de seus conceitos básicos ao setor público;
- a adequada interpretação das bases legais que autorizam o tratamento de dados pessoais;
- os requisitos e as formalidades a serem observados nas hipóteses de uso compartilhado de dados pessoais; e
- a relação entre as normas de proteção de dados pessoais e o acesso à informação pública.

Abrangência do termo "Poder Público".

O termo "Poder Público" é definido pela LGPD de forma ampla e inclui órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e dos três Poderes (Executivo, Legislativo e Judiciário), inclusive das Cortes de Contas e do Ministério Público. Assim, os tratamentos de dados pessoais realizados por essas entidades e órgãos públicos devem observar as disposições da LGPD, ressalvadas as exceções previstas no art. 4º da lei.

Também se incluem no conceito de Poder Público:

- os serviços notariais e de registro (art. 23, § 4º); e
- as empresas públicas e as sociedades de economia mista (art. 24), neste último caso, desde que não estejam atuando em regime de concorrência; ou operacionalizem políticas públicas, no âmbito da execução destas.

Princípios da LGPD.

- **finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- **adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

- **necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- **livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- **transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- **responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Bases Legais da LGPD.

Uma das principais providências a serem tomadas antes de realizar o tratamento de dados pessoais é a de identificar a base legal aplicável. O tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no **art. 7º** ou, no caso de dados sensíveis, no **art. 11** da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos

no **art. 23**, que complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público.

Bases Legais Art. 7º.

- mediante o fornecimento de consentimento pelo titular;
- para o cumprimento de obrigação legal ou regulatória pelo controlador;
- pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
- para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
- quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Bases Legais Art. 11

- quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem).

e) proteção da vida ou da incolumidade física do titular ou de terceiros;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no **art. 9º** desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Considerando os questionamentos encaminhados à ANPD e as peculiaridades do tratamento de dados pessoais pelo Poder Público, bem como o previsto na Agenda Regulatória do biênio 2021–2022, a análise será limitada às seguintes **bases legais**: consentimento, legítimo interesse, cumprimento de obrigação legal e regulatória e execução de políticas públicas.

Consentimento

Conforme a definição legal (art. 5º, XII, LGPD), o consentimento é a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. Adicionalmente, no caso de dados sensíveis, o consentimento deve ser fornecido “de forma específica e destacada, para finalidades específicas” (art. 11, i, LGPD).

Assim, a autorização do titular deve ser intencional e ele deve saber exatamente para que fim seus dados serão tratados, sendo vedada a autorização tácita e para finalidades genéricas. Além disso, o consentimento pressupõe uma escolha efetiva

entre autorizar e recusar o tratamento dos dados pessoais, incluindo a possibilidade de revogar o consentimento a qualquer momento.

Diante dessas características, em muitas ocasiões, o consentimento não será a base legal mais apropriada para o tratamento de dados pessoais pelo Poder Público, notadamente quando o tratamento for necessário para o cumprimento de obrigações e atribuições legais.

Nesses casos, o órgão ou a entidade exerce prerrogativas estatais típicas, que se impõem sobre os titulares em uma relação de desbalanceamento de forças, na qual o cidadão não possui condições efetivas de se manifestar livremente sobre o uso de seus dados pessoais.

Não obstante, o consentimento poderá eventualmente ser admitido como base legal para o tratamento de dados pessoais pelo Poder Público. Para tanto, a utilização dos dados não deve ser compulsória e a atuação estatal não deve, em regra, basear-se no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais.

Assim, a utilização da base legal do consentimento no âmbito do tratamento de dados pessoais pelo Poder Público pressupõe assegurar ao titular a efetiva possibilidade de autorizar ou não o tratamento de seus dados, sem que de sua manifestação de vontade resultem restrições significativas à sua condição jurídica ou ao exercício de direitos fundamentais.

A base legal do consentimento é muito vulnerável por vários motivos já mencionados e quando estamos em processo de inovação, transformação digital, agir com cautela e entender a finalidade correta do tratamento de dados que será realizado é primordial, evita problemas administrativos e jurídicos.

Legítimo Interesse

A base legal do legítimo interesse autoriza o tratamento de dados pessoais de natureza não sensível quando necessário ao atendimento de interesses legítimos do controlador ou de terceiros, “exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais” (art. 7º, IX). **Trata-**

se, portanto, de base legal não aplicável ao tratamento de dados pessoais sensíveis.

Por ser uma base legal mais flexível, sua adoção deve ser precedida de uma avaliação em que seja demonstrada a proporcionalidade entre, de um lado, os interesses do controlador ou de terceiros para a utilização do dado pessoal e, de outro, os direitos e as legítimas expectativas do titular. Além disso, deve-se considerar que, conforme o art. 18, § 2º, o titular tem o **direito de se opor** ao tratamento realizado com base no legítimo interesse, em caso de descumprimento dos requisitos previstos na LGPD.

De forma similar ao que ocorre com o consentimento, a aplicação do legítimo interesse é limitada no âmbito do setor público. Em particular, a sua utilização não é apropriada quando o tratamento de dados pessoais é realizado de forma compulsória ou quando for necessário para o cumprimento de obrigações e atribuições legais do Poder Público.

O legítimo interesse poderá eventualmente ser admitido como base legal para o tratamento de dados pessoais pelo Poder Público. Para tanto, **a utilização dos dados não deve ser compulsória** ou, ainda, a atuação estatal não deve se basear no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais. Nesse contexto, torna-se efetivamente possível realizar uma ponderação entre, de um lado, os interesses legítimos do controlador ou de terceiro e, de outro, as expectativas legítimas e os direitos dos titulares.

Cumprimento de obrigação legal ou regulatória

Conforme o art. 7º, ii, da LGPD, o tratamento de dados pessoais pelo Poder Público poderá ser realizado “para o cumprimento de obrigação legal ou regulatória pelo controlador”. A mesma hipótese está prevista no art. 11, ii, a, que rege o tratamento de dados sensíveis.

De forma geral, a aplicação desses dispositivos será efetuada em dois contextos normativos distintos, que se diferenciam em razão da espécie de norma jurídica que estabelece a obrigação a ser cumprida. É o caso, em especial, das **normas de conduta** e das **normas de organização**.

Execução de políticas públicas

O inciso III do art. 7º da LGPD estabelece que a "administração pública" pode realizar "o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres". Por sua vez, em relação aos dados sensíveis, o art. 11, ii, b, refere-se ao "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos".

A aplicação dessa base legal por entidades e órgãos públicos pressupõe a adequada compreensão sobre os principais termos utilizados nos artigos da LGPD:

- administração pública; e
- políticas públicas.

Compartilhamento de Dados Pessoais

O compartilhamento de dados pessoais é a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública.

De forma mais específica, a LGPD utiliza o termo "**uso compartilhado de dados**", que é definido como a "comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados."

O uso compartilhado de dados é um mecanismo relevante para a execução de atividades típicas e rotineiras do Poder Público, a exemplo de pagamento de servidores e prestação de serviços públicos. A LGPD reconhece essa relevância ao estabelecer, em seu art. 25, que os dados devem ser mantidos "em formato interoperável e estruturado para o uso compartilhado", visando, entre outras finalidades, "à execução de políticas públicas, à prestação de serviços públicos, à

descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral".

Não obstante, assim como ocorre com as demais operações de tratamento, o uso compartilhado de dados pessoais deve ser realizado em conformidade com a LGPD, notadamente com os princípios, as bases legais, garantia dos direitos dos titulares e outras regras específicas aplicáveis ao Poder Público. Além de conferir maior previsibilidade, transparência e segurança jurídica ao uso compartilhado de dados, a observância dessas disposições legais constitui peça-chave para a promoção de uma relação de confiança com os titulares e para a adequada gestão de riscos pelos controladores, inclusive para evitar a ocorrência de abusos e desvios de finalidades.

Divulgação de Dados Pessoais

No setor público, o processo de adequação às disposições da LGPD tem suscitado muitas dúvidas a respeito dos parâmetros a serem observados para a disponibilização pública de informações pessoais. De forma geral, a análise dessas situações envolve uma ponderação entre direitos: de um lado, o direito à privacidade e o direito

à proteção de dados pessoais e, de outro, o direito de todos os indivíduos à informação sobre as atividades do Poder Público.

Este último se traduz, por exemplo, na divulgação, com base no interesse público, de informações relativas à execução de políticas públicas e ao exercício de competências legais pelos órgãos e entes públicos que permitam aos cidadãos o exercício do controle social sobre as atividades do Poder Público.

Frequentemente, todavia, para atender ao princípio da publicidade, o **Estado é obrigado a divulgar dados pessoais**.

Enquanto o primeiro conjunto de direitos demanda uma posição de cautela e de análise de riscos a respeito da divulgação de informações pessoais, o segundo espelha a determinação legal de que a publicidade é a regra, admitindo-se o sigilo apenas em hipóteses excepcionais, nos termos da Lei de Acesso à Informação (**Lei nº 12.527, de 17 de novembro de 2011 – LAI**).

Não obstante, o tratamento de dados pessoais pelo Poder Público, incluindo a divulgação pública de dados pessoais, deve ser realizado em conformidade com as

disposições da LGPD. Mais especificamente, devem ser observadas as normas que garantem a proteção integral dos dados pessoais, a **autodeterminação informativa** e o respeito à privacidade dos titulares durante todo o ciclo do tratamento.

Desde a realização da coleta até o fim da atividade realizada com os dados pessoais, conforme o caso, entidades e órgãos públicos devem, pelo menos, observar os princípios previstos na lei, verificar a base legal aplicável ao tratamento, garantir os direitos dos titulares e adotar medidas de prevenção e segurança, a fim de evitar a ocorrência de incidentes.

O cumprimento da LGPD demanda de entidades e órgãos públicos uma análise mais ampla, que não se limita à atribuição de sigilo ou de publicidade a determinados dados pessoais – este nem mesmo é o escopo da LGPD.

Em termos práticos, considerando o reforço protetivo trazido pela LGPD ao titular de dados, é necessário realizar uma avaliação sobre os riscos e os impactos para os titulares dos dados pessoais bem como sobre as medidas mais adequadas para mitigar possíveis danos decorrentes do tratamento de dados pessoais.

Dados pessoais sensíveis (art. 5º, II, LGPD), por exemplo, estão submetidos a uma proteção jurídica especial, o que implica adotar maior cautela quando for necessário realizar o tratamento de dados pessoais dessa natureza. Nessa linha, pode ser mencionada a vedação de serem revelados dados pessoais sensíveis por ocasião da divulgação de resultados de estudos em saúde pública (art. 13, § 1º, LGPD).

Os princípios da finalidade, adequação e necessidade também impõem limites ao tratamento de dados pessoais. Em atenção a esses princípios, entidades e órgãos públicos devem verificar se as informações coletadas são, efetivamente, adequadas e necessárias para o atendimento das finalidades para as quais serão utilizadas, não podendo haver, desses dados, uso incompatível com as finalidades que justificaram sua coleta ou a sua obtenção.

Muitas vezes, a coleta indiscriminada de dados pessoais é o ponto principal a ser considerado, de modo que, ao invés de eventual e posterior atribuição de sigilo, a proteção será mais efetiva com a própria dispensa da coleta ou com a eliminação da informação.

Em outras situações, nas quais a coleta seja necessária e não seja cabível a eliminação dos dados, podem ser adotadas medidas de mitigação de risco, que fortalecem e tornam mais segura a possibilidade de divulgação dos dados pessoais, haja vista a diminuição de seu potencial lesivo aos direitos dos titulares.

Eventualmente, essas medidas podem ser descritas em relatório de impacto à proteção de dados pessoais, documento do controlador que "contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (arts. 5º, XVII e 38, parágrafo único).

Uma possível salvaguarda a ser adotada é a limitação da divulgação àqueles dados efetivamente necessários para se alcançar os propósitos legítimos e específicos em causa, observados o contexto do tratamento e as expectativas legítimas dos titulares.

Nesse sentido, em cumprimento à decisão proferida pelo STF, a divulgação da remuneração individualizada de servidores públicos federais é realizada sem a apresentação completa de números como o CPF e a matrícula do servidor.

A restrição de acesso a essas informações mitiga os riscos aos titulares de dados pessoais, sem, no entanto, comprometer a finalidade de garantia de transparência e de controle social sobre as despesas públicas. O contexto e as expectativas legítimas dos titulares também são relevantes, na medida em que se entende, como uma decorrência natural do exercício da atividade pública, que determinadas informações pessoais dos servidores se submetam ao escrutínio da sociedade.

Em atenção aos princípios da segurança, da prevenção e da responsabilização e prestação de contas, órgãos e entidades públicas devem adotar medidas técnicas e administrativas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, observado o disposto nos arts. 46 a 49 da LGPD.

Conforme o art. 50, § 1º, constitui boa prática realizar o tratamento de dados pessoais levando em consideração a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados. **Entre outras medidas, sempre que possível, os dados pessoais devem ser pseudonimizados ou anonimizados**.

Mesmo nos casos de divulgação pública de dados pessoais, é recomendável que órgãos e entidades públicos avaliem a possibilidade de adoção de medidas técnicas e administrativas capazes de mitigar riscos e prevenir a ocorrência de danos aos titulares.

Essas medidas adicionais se justificam, pois, em conformidade com os princípios acima referidos, a LGPD estabelece ampla proteção aos dados pessoais, inclusive para aqueles cujo acesso é público, seja por força de lei ou por manifestação de vontade do titular, conforme se extrai de seu art. 7º, §§ 3º, 4º e 7º.

Em algumas situações, a simples atribuição de sigilo aos dados pessoais pode ser uma medida insuficiente para a sua proteção efetiva.

Daí que, em razão da gravidade dos riscos envolvidos em um tratamento e a fim de evitar a ocorrência de incidentes de segurança, pode ser necessária a adoção de mecanismos adicionais de proteção.

É o que ocorre, por exemplo, nos casos de estudos em saúde pública, em relação aos quais o art. 13 da LGPD prevê a adoção de medidas adicionais de prevenção e segurança para o tratamento de dados sensíveis, tais como o seu armazenamento em ambiente controlado e seguro, bem como, sempre que possível, a sua anonimização ou pseudonimização.

A transparência a respeito dos tratamentos de dados realizados e a efetiva garantia de direitos aos titulares devem ser considerados como fatores relevantes para diminuir o uso indevido de dados pessoais. Afinal, a possibilidade de o interessado apresentar um requerimento ao órgão público responsável, relatando eventual violação a seus direitos, pode viabilizar a correção de erros, bem como a implementação de medidas como a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (art. 18, IV).

Responsabilidades envolvendo a Proteção de Dados Pessoais

Solidária = Responsabilidade solidária é quando mais de uma pessoa ou entidade é responsável por uma mesma dívida ou obrigação.

Os Agentes de tratamento de dados pessoais (Controlador e Operador) respondem de forma solidária em caso de dano ou prejuízo causado a titular de dados pessoais.

A responsabilização pode acontecer na esfera: Administrativa e ou Jurídica.

Encarregado de Proteção de Dados - DPO

O Encarregado pelo Tratamento de Dados Pessoais (**DPO**) surge com o advento da Lei nº 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). O art. 5º, inciso VIII, da LGPD o conceituou como a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".

Além de funcionar como canal de comunicação, segundo o art. 41, inciso III, da LGPD, cabe também ao encarregado "orientar os funcionários e os contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais."

Governança e Educação Digital

Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - Implementar programa de governança em privacidade que, no mínimo:

- demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
- conte com planos de resposta a incidentes e remediação; e
- seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - Demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

Sanções Administrativas

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- multa diária, observado o limite total a que se refere o inciso II;
- publicização da infração após devidamente apurada e confirmada a sua ocorrência;

- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Pontos Importantes da LGPD

As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

- a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- a boa-fé do infrator;
- a vantagem auferida ou pretendida pelo infrator;
- a condição econômica do infrator;
- a reincidência;
- o grau do dano;
- a cooperação do infrator;
- a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
- a adoção de política de boas práticas e governança;
- a pronta adoção de medidas corretivas; e
- a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

8.0 - PRESERVAÇÃO DIGITAL SISTÊMICA

Desde a invenção da escrita que existe uma manifesta preocupação pela preservação dos artefatos que resultam de processos intelectuais e criativos do ser humano. A preservação desses artefatos permite às gerações futuras compreenderem e contextualizar a história e a cultura dos seus povos. Os museus, as bibliotecas e os arquivos assumem neste contexto um papel determinante, responsabilizando-se pela preservação e longevidade desses artefatos.

Nos dias de hoje, uma parte significativa da produção intelectual é realizada com o auxílio de ferramentas digitais.

O curso da história tem revelado inúmeros exemplos fatídicos de obsolescência tecnológica.

- VHS
- Disquetes
- CDs

A obsolescência tecnológica não se manifesta somente ao nível dos suportes físicos. No domínio digital, todo o tipo de material tem obrigatoriamente de respeitar as regras de um determinado formato. Isto permite que as

aplicações de software sejam capazes de abrir e interpretar adequadamente a informação armazenada. À medida que o software vai evoluindo, também os formatos por ele produzidos vão sofrendo alterações.

No mundo atual, onde cada vez mais organizações dependem da informação digital que produzem, torna-se premente a implementação de técnicas e de políticas concertadas que vão no sentido de garantir a perenidade e a acessibilidade a este tipo de informação.

Designa-se, assim, por **PRESERVAÇÃO DIGITAL** o conjunto de atividades ou processos responsáveis por garantir o acesso continuado a longo-prazo à informação e restante património cultural existente em formatos digitais.

A preservação digital consiste na capacidade de garantir que a informação digital permanece acessível e com qualidades de autenticidade suficientes para que possa ser interpretada no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da sua criação.

Objeto Digital

Um o **Objeto Digital** pode ser definido como todo e qualquer objeto de informação que possa ser representado através de uma sequência de dígitos binários. Esta definição é suficientemente para acomodar tanto, informação nascida num contexto tecnológico digital (**objetos nato-digitais**), como informação digital obtida a partir de suportes analógicos (**objetos digitalizados**).

Documentos de texto, fotografias digitais, diagramas vectoriais, bases de dados, sequências de vídeo e áudio, modelos de realidade virtual, páginas Web e aplicações de software são apenas alguns exemplos do que podemos considerar um objeto digital.

Para que um ser humano seja capaz de decifrar um objeto digital, há um conjunto de transformações que têm necessariamente de ocorrer.

Um objeto digital começa por ser um objeto físico: um conjunto de símbolos ou sinais inscritos em diferentes suportes físicos e formatos, para o mesmo tipo de objeto.

Exemplo: Uma fotografia pode ser alocada em qualquer suporte de armazenamento em formato: JPEG, PNG etc.

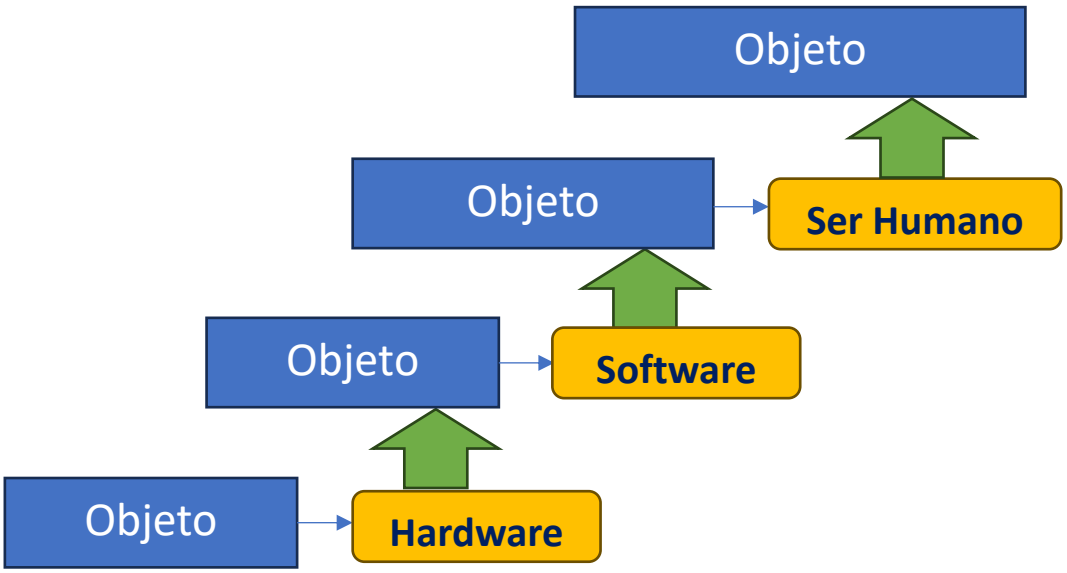
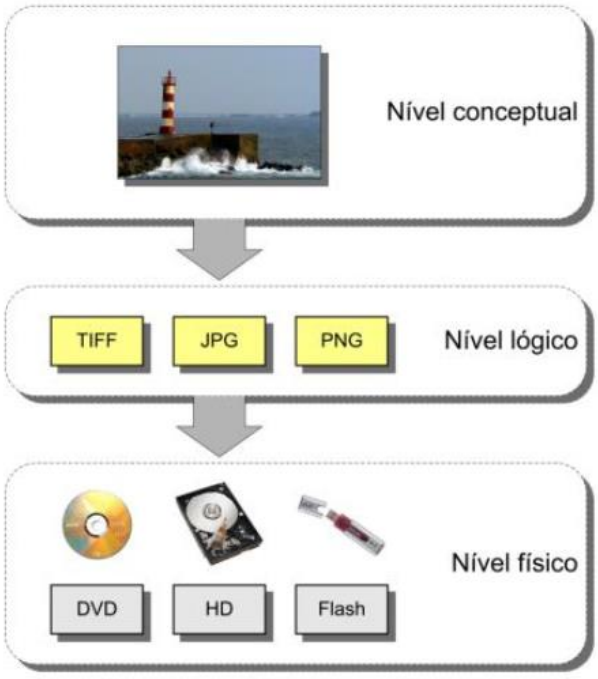


Figura 1: Níveis de Abstração

Fonte: Própria



Documento manifestado: se apresenta de maneira compreensível ao usuário final;

Codificação em Bits;

Suporte Físico

Figura 2: Níveis de Abstração

Fonte: MÁRDERO ARELLANO, Miguel Ángel. Introdução à preservação digital – Conceitos, estratégias e actuais consensos. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006.

Numa situação ideal, o objeto conceptual formado na mente do emissor será em tudo semelhante ao objeto conceptual concebido pelo receptor. Somente nessa situação a comunicação poderá ser considerada perfeita.

A preservação digital é a atividade responsável por garantir que a comunicação entre um emissor e um receptor é possível, não só através do espaço, mas também através do tempo.

Para que a preservação de um objeto digital seja possível, é necessário assegurar que todos os níveis de abstração anteriormente descritos se encontram acessíveis e interpretáveis. Se a cadeia de interpretação que permite elevar um objeto digital desde o seu nível físico até o nível conceptual for rompida, a comunicação deixa de ser possível e o objeto perder-se-á para sempre.

Preservação Digital

Pode ser definida como o "planejamento, alocação de recursos e aplicação de métodos e tecnologias para assegurar que a informação digital permaneça acessível e utilizável ao longo do tempo." (Hedstrom, 1996, apud ARELLANO, 2008, p.43).

Engloba mecanismos de armazenamento, gerenciamento de objetos digitais, estratégias metodológicas e parâmetros de arquivamento. (MÁRDERO ARELLANO, 2008, p.41).

A preservação digital pode contribuir para:

- Garantir a confiabilidade, a autenticidade e a acessibilidade das informações contidas nos documentos.
- Evitar a perda de um simples "dígito binário" (bit, menor unidade de informação que pode ser armazenada ou transmitida), que pode ser catastrófica !
- Reduzir as consequências da obsolescência tecnológica de Hardware e/ou Software).
- Garantir a recuperação a longo prazo das informações.
- Os documentos (cópias) podem ser facilmente reproduzidos, preservando a documentação física.
- Múltiplos acessos. Os mesmos recursos podem ser usados ao mesmo tempo por vários usuários.

- Preservar informações que temos certeza de que serão necessárias no futuro.
- Para fins legais, fiscais, testemunho, memória e patrimônio.
- Capacidade de garantir que os documentos nato-digitais ou digitalizados permaneçam autênticos, acessíveis e utilizáveis ao longo do tempo;
- A capacidade de reproduzir documentos, imagens, vídeos ou sons de uma forma suficientemente semelhante ao original;
- A capacidade de compreender um conjunto de dados e utilizá-lo em ferramentas de análise para gerar resultados.

Ameaças a preservação dos documentos digitais:

- “Fragilidade” dos documentos digitais;
- Mídias e hardware obsoletos (falhas, deterioração etc.);
- Softwares são atualizados ou descontinuados;
- Ataques cibernéticos;
- Ausência da cadeia de custódia;
- Aumento exponencial de documentos e informações (Gestão);
- Perda da memória histórica e de documentos probatórios;
- Sistema de Gestão, Backup, Storage, Certificado Digital e Antivírus não garantem a preservação.

O processo de preservação digital precisa ser planejado, implantado e sustentável.

Elementos da preservação digital

São elementos da preservação digital os seguintes elementos:

- Elementos Organizacionais
- Elementos Legais
- Elementos Técnicos

Elementos Organizacionais tem como características:

- Objetivos da Instituição
- Equipe Multidisciplinar

- Responsabilidades
- Recursos Financeiros

Elementos Legais tem como características:

- Leis
- Direitos Autorais
- Atos Administrativos

Elementos Técnicos tem como características:

- Autenticidade
- Seleção e Descarte
- Modelos e Padrões
- Metadados
- Infraestrutura Tecnológica
- Repositórios Institucionais
- Estratégias de Preservação
- Iniciativas e Parcerias
- Acesso
- Auditoria e Certificação

O MODELO OAIS

A **ISO 14721:2003** especifica os principais critérios nos quais iniciativas em preservação digital devem se amparar e resulta no modelo de referência OAIS (Open Archival Information System).

No Brasil, foi adaptado e publicado como norma **ABNT NBR 15472: 2007**, sob o título "Sistema Aberto de Arquivamento de Informação – SAAI", substituída pela **NBR ISO 14721:2021** de mesma titulação.

Modelo OAIS - ISO 14721 (versão 2024)

Modelo de Referência para um Sistema Aberto de Arquivamento de Informações (OAIS).

NORMA ISO 16363

Auditoria e Certificação dos RDC's - Repositórios Digitais Confiáveis

NORMA ISO 16919

Requisitos para Organizações de Auditoria e Certificação baseada na ISO 16363

A **ISO 14721:2003** especifica os principais critérios nos quais iniciativas em preservação digital devem se amparar e resulta no modelo de referência OAIS (Open Archival Information System).

No Brasil, foi adaptado e publicado como norma **ABNT NBR 15472: 2007**, sob o título "Sistema Aberto de Arquivamento de Informação – SAAI", substituída pela **NBR ISO 14721:2021** de mesma titulação.

Modelo funcional conceitual que estrutura e orienta um repositório digital para que este realize a manutenção e a preservação das informações digitais por um longo período.

O Modelo de Informação do OAIS propõe o conceito de pacotes de informação:

- Submission information package (SIP);
- Archival information package (AIP);
- Dissemination information package (DIP).

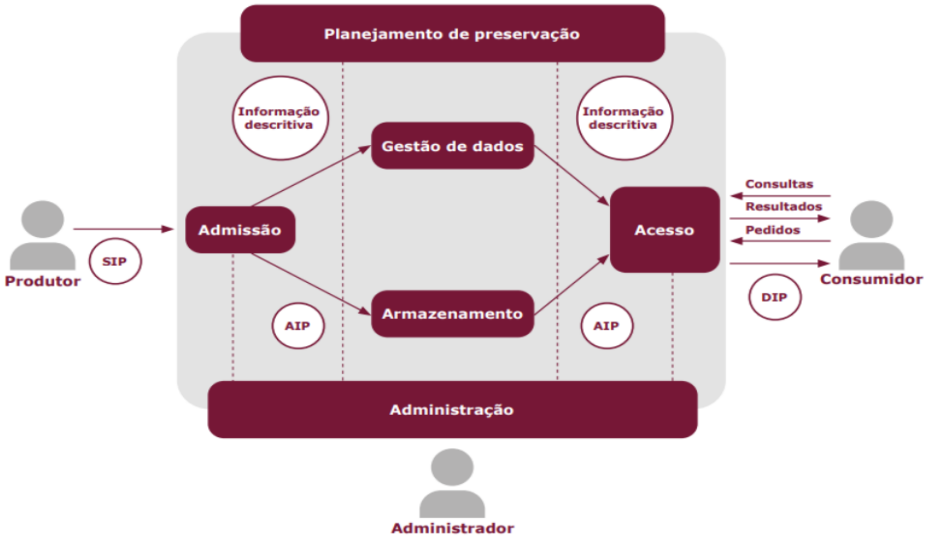


Figura 3: Preservação Digital

Fonte: CONARQ - DIRETRIZES PARA IMPLEMENTAÇÃO DE REPOSITÓRIOS ARQUIVÍSITICOS DIGITAIS CONFIÁVEIS – RDC-ARQ

O **PRODUTOR** deverá ser entendido como a entidade externa ao repositório que se responsabiliza pela submissão de material. O material submetido a arquivo é aqui representado pelo pacote de submissão (SIP).

Durante o processo de submissão, o repositório é responsável por **garantir a integridade** da informação recebida. Ainda nesta fase, é produzida toda **informação descritiva** que irá suportar a descoberta e localização do material depositado. Essa informação descritiva (metadados) é armazenada e gerida pelo componente **Gestão de Dados**. O documento será preservado no Repositório (Armazenamento – em formato AIP).

O componente **Planejamento de Preservação** encarrega-se da definição de políticas de preservação. Este serviço é responsável pela monitorização do ambiente externo ao repositório e por desencadear eventos de preservação sempre que necessário. É, por exemplo, da responsabilidade deste componente definir as estratégias de preservação a utilizarem no interior do repositório, monitorizar as tendências comportamentais da sua comunidade de interesse ou identificar formatos que se encontram na iminência de se tornar obsoletos.

O componente **Acesso** estabelece a ponte entre o repositório e a sua comunidade de interesse, o conjunto de potenciais **Consumidores** do material custodiado. Este componente é responsável por facilitar a descoberta e localização dos objetos digitais, bem como preparar os mesmos para entrega ao consumidor.

Os pacotes que são entregues ao consumidor assumem a forma de Pacotes de Informação de Disseminação (DIP).

O DIP sempre será diferente do AIP.

A informação que é entregue ao consumidor poderá ser apenas um subconjunto da informação arquivada ou até uma versão transformada.

Por último, o componente **Administração** é responsável pelas operações diárias de manutenção e sobretudo pela parametrização e monitorização dos processos desencadeados no interior do repositório. Este componente interage com todos os restantes de modo a assegurar o correto funcionamento.

Vivemos em uma sociedade cada vez mais digital. E essa digitalização tem proporcionado benefícios para os consumidores – e transformado indústrias.

Ao mesmo tempo, transformar digitalmente uma empresa ou instituição implica afrontar vários desafios, entre eles o fato de que a disrupção causada pelo digital está se acelerando e, em alguns casos, levando a dinâmicas de mercado em que poucos são os líderes que terminam concentrando a maior fatia do mercado.

Quando se trata de “digital”, no entanto, procurar seguir as principais tendências com velocidade parece não ser suficiente . A prova disso é a constatação de que, mesmo em setores altamente digitalizados, a maturidade digital pode variar significativamente de forma a impactar os resultados das empresas – líderes em maturidade digital no mundo apresentam desempenho superior com taxa de crescimento de EBITA até 5 vezes maior em comparação às demais empresas.

Mas, o que é “digital”? Transformações digitais podem ser caracterizadas por acionar ao menos uma de quatro alavancas-chave de valor: **(i)** Modelos de negócio (novas formas de operar e novos modelos econômicos); **(ii)** Conectividade (engajamento em tempo real); **(iii)** Processos (foco na experiência do cliente, automação e agilidade) e **(iv)** Analytics (melhor tomada de decisão e cultura de dados). No entanto, para capturar o valor criado por essas alavancas, é necessário associá-las a um conjunto de melhores práticas de gestão que abrangem quatro dimensões fundamentais: Estratégia, Capacidades, Organização e Cultura.

A maturidade digital de uma empresa no setor público ou privado pode contribuir para um maior crescimento e sucesso, mas qual é a realidade das principais empresas do Brasil neste aspecto?

- Reunir em grupos (números de participantes serão definidos conforme a quantidade em sala).
- Descrever pontos de vista sobre o questionamento.

9.0 - CITAÇÕES E REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DADOS (ANPD). Guia orientativo de Tratamento de Dados Pessoais pelo Poder Público. Versão 2.0. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 26/02/2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 30300:2016: Informação e documentação — Sistema de gestão de documentos de arquivo —Fundamentos e vocabulário. Rio de Janeiro, 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 15489-1:2018: Informação e documentação — Gestão de documentos de arquivo Parte 1: Conceitos e princípios. Rio de Janeiro, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 16167:2020: Segurança da informação — Diretrizes para classificação, rotulação, tratamento e estão da informação. 2ª ed. Rio de Janeiro, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. 3ª ed. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002:2022: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. 3ª ed. Rio de Janeiro, 2022.

BRASIL. Lei nº 8.159, de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8159.htm. Acesso em: 26/12/2024.

BRASIL. Lei Nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 26/12/2024.

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 26/12/2024.

BRASIL. Lei nº 8.159, de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8159.htm. Acesso em: 26/12/2024.

CHRISTENSEN, Clayton M. , HORN, Michael B., STAKER, Heather. Ensino Híbrido: uma Inovação Disruptiva? Uma introdução à teoria dos híbridos. Traduzido para o Português por Fundação Lemann e Instituto Península. Maio de 2013. Disponível em: https://www.pucpr.br/wp-content/uploads/2017/10/ensino-hibrido_uma-inovacao-disruptiva.pdf. Acesso em: 26/12/2024.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ) - Resoluções do CONARQ. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq

CONSELHO NACIONAL DE ARQUIVOS (Brasil). e-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. [recurso eletrônico] / Câmara Técnica de Documentos Eletrônicos. 2. versão. – Dados eletrônicos (1 arquivo : 1 MB). Rio de Janeiro: Arquivo Nacional, 2022. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/EARQV203MAI2022.pdf. Acesso em: 28/12/2024.

CONSELHO NACIONAL DE JUSTIÇA. Modelo de requisitos para sistemas informatizados de gestão de processos e documentos do Poder Judiciário: MoReqJus / Conselho Nacional de Justiça – 2 ed. – Brasília: CNJ, 2023. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2023/10/moreq-jus-2a-edicao.pdf. Acesso em: 28/12/2024.

FLORES, Daniel. A transformação digital compulsória que vem acometendo os arquivos, os documentos e arquivistas. quais subsídios temos para uma tomada de decisão: disruptiva ou inovação sustentada? Por Daniel Flores, Representante de Brasil en el GE RIBEAU ALA, Editorial para o Boletim Informativo da ALA. Disponível em: https://www.alaarchivos.org/wp-content/uploads/2022/03/Artigo-Daniel-Flores.pdf. Acesso em: 26/12/2024.

FLORES, D. Cadeia de custódia digital de documentos arquivísticos: do Sigad ao RDC-Arq. Brasília, DF: Instituto de Patrimônio Histórico e Artístico Nacional (Iphan), 2016, 122 slides, color, padrão slides Google Drive/Docs 4x3. Material elaborado para a palestra no Iphan, 28 abr. 2016. Disponível em: <http://documentosdigitais.blogspot.com>. Acesso em: 03/02/2025.

FLORES, D.; Rocco, B. C. B.; Santos, H. M. D. Cadeia de custódia para documentos arquivísticos digitais. Acervo - Revista do Arquivo Nacional, v. 29, n. 2, p. 117-132, 2016. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/40511>. Acesso em: 03/02/2025.

FONTANA, F. F.; Flores, D.; Nora, F. D.; Santos, H. M. D. Archivematica como ferramenta para acesso e preservação digital à longo prazo. Ágora, v. 24, n. 48, p. 62-82, 2014. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/13494>. Acesso em: 03/02/2025.

FERREIRA, Miguel, Introdução à preservação digital – Conceitos, estratégias e actuais consensos. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006.

HENRIETTE, E., FEKI, M. & BOUGHZALA, I., 2015, 'The shape of digital transformation: Assistemática literature review', Ninth Mediterranean Conference on Information Systems (MCIS), Samos,3rd–5th October 2015. South African Journal of Economic and Management Sciences. Available from: https://www.researchgate.net/publication/359004477_South_African_Journal_of_Economic_and_Management_Sciences. Acesso em: 03/02/2025.

INNARELLI, H. C. Gestão da preservação de documentos arquivísticos digitais: proposta de um modelo conceitual. 2015. Tese (Doutorado em Cultura e Informação) - Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2015.

MÉNDEZ, S. G.; ANDREU, T. A.; TIRADOR, J. L. Transformação digital: a arte de pensar como uma Startup. Madrid: Desenvolvendo ideias, 2015.

RONDINELLI, R. C. O documento arquivístico ante a realidade digital: uma revisão necessária. 2011, 270f. Tese(Doutorado em Ciência da Informação) – Universidade Federal Fluminense, PPGCI/IBICT, Niterói, 2011.