REVISTA DE GESTÃO E SECRETARIADO
MANAGEMENT AND ADMINISTRATIVE PROFESSIONAL REVIEW
ISSN: 2178-9010

Revista GeSec
São Paulo, SP, Brasil
v. 14, n.3, p. 2836-2856,
2023

DOI: http://doi.org/10.7769/gesec.v14i3.1753

Gestão arquivística e administração pública: a preservação e a segurança dos documentos arquivísticos digitais

Archival management and public administration: the preservation and security of digital archival documents

Josimas Eugênio Silva[1]
Thiago Thito de Paula Oliveira Neves[2]
Michael David de Souza Dutra[3]
Gustavo Henrique Petean[4]

Resumo

Diante da multiplicação da informação nos últimos anos, resultado da globalização e dos avanços tecnológicos, o presente estudo promoveu uma revisão da literatura na busca de métodos existentes para a preservação e segurança dos documentos arquivísticos digitais, a fim de garantir seu futuro acesso, bem como a sua autenticidade e integridade em longo prazo. Dessa forma, neste estudo pretendeu-se identificar a causa das deficiências na preservação dos documentos arquivísticos digitais, bem como propor possíveis soluções para os mesmos. Para tanto, foram utilizados os métodos de pesquisa bibliográfica e exploratória como procedimentos técnicos, com abordagem qualitativa, relacionados à gestão documental e à preservação de documentos digitais. Buscou-se ainda, como base conceitual, analisar a Lei de

[1] Pós-graduação em Controle Externo e Governança Pública pelo Instituto Brasiliense de Direito Público (IDP). E-mail: josimaseugenio@discente.ufg.br Orcid: https://orcid.org/0000-0002-7188-0493
[2] Especialista em Docência Universitária pela Faculdade Católica de Anápolis, R. Quatorze de Julho, 830, Centro, Anápolis - GO, CEP: 75024-050. E-mail: thiagothito@ufg.br
Orcid: https://orcid.org/0000-0001-9293-8810
[3] Doutor em Matemática Aplicada para Engenheiros, Polytechnique de Montreal, Canadá, 2500, Chem. de Polytechnique, Montréal, QC H3T 1J4, Canadá. E-mail: michaeldavid@ufg.br
Orcid: https://orcid.org/0000-0003-4500-5510
[4] Doutor em Administração pela Universidade Federal de Mato Grosso do Sul, Cidade Universitária, Av. Costa e Silva, Pioneiros - MS, CEP: 79070-900. E-mail: gustah@ufg.br
Orcid: https://orcid.org/0000-0003-1248-6418

Arquivos, Lei de Acesso à Informação e Lei Geral de Proteção de Dados Pessoais, bem como as diretrizes estabelecidas pelo Conselho Nacional de Arquivos, além de trazer um caso prático para verificação de aplicabilidade dos conceitos tratados neste estudo. Por fim, a pesquisa revela desafios que envolvem a preservação da informação arquivística em meio digital, dentre eles a rápida degradação física dos suportes e a obsolescência tecnológica, bem como propõe a utilização de repositórios arquivísticos digitais confiáveis como uma das soluções para esses problemas.

Palavras-chave: Informação. Digitalização Documentos. Gestão Arquivística. Pesquisa Exploratória.

Abstract

Given the multiplication of information in recent years, a result of globalization and technological advances, this study promoted a literature review in search of existing methods for the preservation and security of digital archival documents in order to ensure their future access, as well as their authenticity and integrity in the long term. In this way, this study aimed to identify the cause of deficiencies in the preservation of digital archival documents, as well as to propose possible solutions. To this end, bibliographic and exploratory research methods were used as technical procedures, with a qualitative approach, related to document management and the preservation of digital documents. We also sought, as a conceptual basis, to analyze the, in the Brazilian case, Law of Archives, the Law of Access to Information and the General Law of Protection of Personal Data, as well as the guidelines established by the National Council of Archives, and to bring a practical case to verify the applicability of the concepts addressed in this study. Finally, the research reveals challenges involving the preservation of archival information in digital media, among them the rapid physical degradation of the media and technological obsolescence, and proposes the use of reliable digital archival repositories as one of the solutions to these problems.

Keywords: Information. Digitization of Documents. Archival management. Exploratory Research.

Introdução

Perante os avanços tecnológicos adicionados à globalização e o uso da internet, percebe-se a multiplicação da informação e o seu crescimento de forma constante, diante de

seu valor probatório, finalidade científica, e seu apoio às atividades do órgão ou entidade custodiadora (Júnior, 2022).

Em paralelo, observa-se uma evolução nos suportes em que essas informações são tratadas e armazenadas, fazendo surgir preocupações para garantir a sua preservação, integridade e autenticidade durante todo o seu ciclo de vida, bem como sua disponibilidade. A falta de informação pode provocar decisões não otimizadas (de Souza Dutra *et al*., 2019), custosas ou sem fundamentos (Carvalho de Sá *et al.*, 2022; de Assis *et al*., 2021). Diante de possíveis problemas como a indisponibilidade da informação e a perda da integridade e autenticidade, possivelmente causadas pelos incidentes de segurança da informação, surge a necessidade de se buscar métodos eficazes para mitigar ou eliminar tais problemas.

Nesse cenário, o presente trabalho objetiva verificar a existência de métodos capazes de promover a preservação da informação arquivística, produzida e custodiada em meio digital por entidades governamentais, bem como verificar a sua possível regulamentação e aplicação, visando diagnosticar soluções para problemas como a obsolescência tecnológica dos suportes e os incidentes de segurança da informação.

Como metodologia, foram utilizados os métodos de pesquisa bibliográfica e exploratória como procedimentos técnicos, com abordagem qualitativa, relacionados à gestão documental, acesso, tratamento de dados e segurança da informação. Buscou-se, ainda, revisar a legislação aplicada ao tema desta pesquisa, prevista na Lei de Arquivos, Lei de Acesso à Informação (LAI) e Lei Geral de Proteção de Dados Pessoais (LGPD), bem como as diretrizes estabelecidas pelo Conselho Nacional de Arquivos-CONARQ, a fim de se verificar a existência de padrões pré-estabelecidos que disciplinem a temática, e também a utilização de dados secundários e análise de periódicos.

Como resultados, discute-se o conceito e a finalidade dos arquivos públicos, cujas atividades estão regulamentadas pela Lei 8.159/91 (Lei de Arquivos), que trata da política nacional de arquivos públicos e privados no Brasil, dentre outras disposições. Ainda, foram discutidos os possíveis problemas quanto à preservação da informação arquivística diante da falta de requisitos para o seu tratamento, bem como uma forma de conscientizar os responsáveis pelas operações de guarda sobre as possíveis consequências da obsolescência dos suportes e dos incidentes de segurança da informação.

Na primeira seção, são debatidos os assuntos que norteiam o conhecimento sobre os arquivos públicos por meio da Lei de Arquivos, Lei de Acesso à Informação e Lei Geral de Proteção de Dados, e em seguida, na próxima seção, abordam-se os conceitos do tratamento de dados realizados pelo poder público, e por fim, na última seção, trata-se da preservação da

informação arquivística digital, demonstrando os métodos e práticas que devem ser aplicados no tratamento de dados, trazendo, ainda, como caso prático, a efetivação da segurança da informação proposta pelo Tribunal de Contas do Estado de Goiás.

Referencial Teórico

Visando o alcance dos objetivos propostos, buscou-se, de forma investigativa e exploratória, abordar a temática sobre os arquivos públicos: análise histórica, conceitual e legislação aplicada, passando a fragmentá-la da seguinte forma: os arquivos públicos, a lei de acesso à informação e a lei geral de proteção de dados. Em seguida abordou-se o tratamento de dados realizado pelo poder público, por meio da discussão dos tipos de arquivo e a obrigatoriedade da gestão arquivística, passando a discorrer sobre a preservação e segurança da informação arquivística digital, demonstrando as técnicas na preservação da informação arquivística digital, o repositório digital confiável de documentos arquivísticos: conceito e principais requisitos e por fim sobre os incidentes de segurança da informação.

2.1 Os Arquivos Públicos: Análise Histórica, Conceitual e Legislação Aplicada

2.1.1 Os arquivos públicos

Diante da necessidade de se registrar fatos e coisas, e em conservar esses registros, resquícios encontrados em cavernas remetem a história das civilizações às novas gerações (Hora; Saturnino & Santos, 2010). Porém, com o passar do tempo, as formas de comunicação sofreram várias modificações estruturais, tanto em suas características intrínsecas quanto nas extrínsecas, as quais se transformaram em fontes de pesquisa científica e base legal de informações, promovendo direitos e obrigações (Schwaitzer, 2011). Os arquivos foram criados diante da necessidade das organizações registrarem sua memória, com vistas a harmonizar o funcionamento da coletividade e das instituições, bem como promover seu futuro (Robert, 1990 *apud* Jardim, 1996).

Com a promulgação da Constituição Federal de 1988, mudanças significativas ocorreram em todo contexto nacional, deixando evidente o dever de obediência aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência por parte de toda administração pública direta e indireta, bem como por qualquer dos poderes da União, dos Estados, Distrito Federal e Municípios (Brasil, 2020).

Nesse contexto, a Lei nº 8.159/91, em seu artigo 2º, define "arquivo" como "*conjuntos documentais produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos"* (Brasil, 2022). O Conselho Nacional de Arquivos – CONARQ corrobora a supracitada lei ao definir o arquivo como "*instituição ou serviço que tem por finalidade a custódia, o processamento técnico, a conservação e o acesso aos documentos arquivísticos"* (CONARQ, 2020).

Por fim, na Resolução nº 27/2008 do Conselho Nacional de Arquivos, observa-se o dever do Poder Público, no âmbito dos Estados, do Distrito Federal e dos Municípios, de criar e manter Arquivos Públicos, na sua específica esfera de competência, no sentido de promover a gestão, a guarda e a preservação de documentos arquivísticos e a disseminação das informações neles contidas (CONARQ, 2020).

2.1.2 A Lei de Acesso à Informação

Em meio a uma nova sociedade, atualmente conhecida como sociedade da informação, a qual exerce o monitoramento, coleta de dados com o fim de prever comportamentos, atuando sobre o exame digital da informação (Botelho & Camargo, 2021), a Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI), assim denominada, veio constituir importantes diretrizes para assegurar o direito de acesso do cidadão à informação e aos documentos públicos (Schwaitzer, 2019), para tanto, dispõe sobre os procedimentos a serem executados pelo governo, com o objetivo de garantir o acesso à informação (Brasil, 2019).

Assim, promulgada em 18 de novembro de 2011, considerada como resultado de um esforço da Administração Pública em trazer mais transparência de seus atos, bem como em disponibilizar ao cidadão as informações de caráter público (Brasil, 2022), trata-se de uma lei federal aplicada a toda administração brasileira direta e indireta, e também, às entidades que recebem recursos públicos (Condeixa, 2012), haja vista que a publicidade e a transparência são as principais diretrizes que regem a disponibilização das informações, devendo sempre ser públicas, exceto quando forem consideradas sigilosas (Brasil, 2022).

No que se refere ao tratamento dos dados, a Lei nº 12.527/11, em seu artigo 4º, inciso V, o define como "*um conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento,*

armazenamento, eliminação, avaliação, destinação ou controle da informação" (Brasil, 2019).

2.1.3 A Lei Geral de Proteção de Dados

Em um contexto histórico sobre a criação da Lei Geral de Proteção de Dados – LGPD, observa-se que os assuntos que norteiam proteção de dados começaram a ser debatidos na Alemanha por volta dos anos de 1970, pois, diante dos avanços tecnológicos no tratamento de dados, muitos países aprovaram suas próprias normas com o fim de se estabelecer a proteção de suas informações, (Candido; Araújo & Ribeiro, 2021). Assim, em 2012, na Europa, nasce o Regulamento Geral sobre a Proteção de Dados – GDPR, fonte de inspiração para a aprovação da Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais – LGPD), representando um importante passo no cenário nacional, disciplinando o tratamento de dados pessoais e promovendo a proteção dos direitos fundamentais de liberdade e de privacidade (Botelho & Camargo, 2021).

Figuras como a do controlador, operador e encarregado são trazidas pela nova lei, haja vista a manutenção de registro das operações de tratamento de dados pessoais que possam realizar, bem como aceitar comunicações e reclamações dos titulares, esclarecer dúvidas e adotar outras providências. Nota-se, também que essa lei possui um capítulo específico para normatizar o tratamento de dados pessoais pelo poder público, afirmando que esse tratamento deverá ocorrer para o atendimento de sua finalidade pública, com o objetivo de executar competências ou cumprir atribuições legais do serviço público. Tal lei elenca requisitos para esse tratamento, dentre os quais, que seja indicado um encarregado para a realização de operações de tratamento de dados pessoais (Brasil, 2018).

Nesse contexto, diante do dever de atuar como canal de comunicação entre a instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), é criada a figura do "**Encarregado pelo Tratamento de Dados Pessoais"**, o qual promoverá o acesso das atividades de tratamento de dados pela organização (SERPRO, 2022).

Ademais, no que se referem aos dados, com vistas 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, essa mesma lei afirma que estes dados deverão ser mantidos em formato interoperável e estruturado para o seu uso compartilhado (Brasil, 2018).

2.2 O Tratamento de Dados Realizado pelo Poder Público

2.2.1 Tipos de Arquivo

Antes de adentramos, especificamente, aos assuntos tratados nas demais seções, verificou-se a necessidade de trazer ao estudo, de forma conceitual, os elementos que qualificam e estruturam os arquivos, com o fim de promover um conhecimento prévio sobre essa temática, e ainda, neste contexto, reconhecer a importância dos profissionais de arquivo, haja vista os seus conhecimentos específicos, como o estudo da gênese documental, da diplomática contemporânea e da tipologia documental (Schwaitzer, 2019).

Quando nos referimos à palavra "arquivo" observa-se que os seus diversos significados se integram em perspectivas empíricas, técnicas, científicas e filosóficas, haja vista a sua associação ao conjunto de documentos acumulados e outros artefatos produzidos ou reconhecidos, e que, em seu contexto, registram experiências e atividades vivenciadas (Tavares & Meira Mota, 2020).

Ademais, neste cenário, percebe-se que a Lei nº 8.159/91, art. 7º, traz o conceito de arquivos públicos ao afirmar que são "*conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias"* (Brasil, 2022).

Ressalta-se que esses arquivos são registrados por meio de uma diversidade de suportes, ou seja, o material em que são efetuados os registros, dentre esses, os suportes físicos, por exemplo, papel, filme e fotografias e outros, bem como os suportes digitais, que necessitam de equipamentos eletrônicos para que possam ser acessados, a exemplo disso, os discos óticos, discos magnéticos e outros formatos, os quais promovem o armazenamento digital de áudio ou de dados em meio eletrônico (CONARQ, 2020).

Ao considerar que "*os documentos arquivísticos se constituem, primeiramente, em instrumentos fundamentais para a tomada de decisão e para a prestação de contas de órgãos ou entidades, e, num segundo momento, em fontes de prova, garantia de direitos aos cidadãos e testemunhos de ação"*, espera-se que seja adotado processos para dar acesso contínuo aos documentos e garantia de autenticidade e confiabilidade dos mesmos.

Perante as mudanças ocorridas no tratamento das informações em virtude do surgimento e adoção de novas tecnologias, a produção de documentos em suportes físicos ganhou novo formato, passando a ser produzida em meio eletrônico. Com isso, o seu

armazenamento também ganhou forma digital, fazendo, assim, com que o trabalho dos operadores, responsáveis pelo tratamento da informação, também sofresse uma reestruturação (Schäfer & Constante, 2013).

2.2.2 Obrigatoriedade da Gestão Arquivística

Ainda que exista uma transição no *modus operandi* da gestão arquivística, as instituições, necessitam garantir a gestão e preservação das informações, independentemente do tipo de suporte, contidas em seus acervos arquivísticos, destacando, assim, as instituições públicas, haja vista que essas são responsáveis pela conservação e preservação de documentos e informações pertencentes à sociedade (Schäfer & Constante, 2013). Neste contexto, a Constituição Federal Brasileira, em seu artigo 5º, inciso XXXIII, afirma que todos "*têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, e que estas informações serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado"* (Brasil, 2020).

Ademais a gestão documental, também é conceituada pela Lei nº 8.159/91, em seu art. 3º, como o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente (Brasil, 2022), assim, é necessário que se desenvolvam procedimentos que garantam a gestão dos documentos, bem como a sua preservação e acesso ao longo do tempo, haja vista que as instituições utilizam-se da informação arquivística digital para promoção de suas atribuições (Schäfer & Constante, 2013).

De outro lado, toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, se referem ao tratamento de dados, conforme disposto no artigo 5º, inciso X, da Lei nº 13.709/18 - Lei Geral de Proteção de Dados (Brasil, 2018).

Por fim, ressalta-se que alguns princípios como a finalidade, adequação, necessidade, acesso livre, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização, os quais estão contidos no novo dispositivo legal (LGPD), deverão ser observados pelos órgãos do poder público para que se promova o tratamento dos dados

(SERPRO, 2022), uma vez que a LGPD dilata a abrangência da LAI e estabelece critérios que podem interferir nas atividades de gestão de documentos da administração pública (Belloto, 2002).

2.3 A Preservação e Segurança da Informação Arquivística Digital

Para que se possa avançar nessa temática, se faz necessário saber que a preservação digital é conceituada como um conjunto de estratégias através das quais se definem diretrizes e modelos conceituais e práticos, os quais garantem a perenidade da informação tornando-as acessíveis em longo prazo (Schäfer & Constante, 2013). Assim, com o objetivo de resguardar as informações produzidas em formato impresso para a utilização das novas gerações, em decorrência do nascimento de uma nova era, as inquietações no que se refere à preservação digital se deram ainda no século XX, consequência das vulnerabilidades que ocorrem no meio digital, dentre elas a rápida degradação física, a obsolescência tecnológica, a complexidade e os custos elevados de manutenção (Nascimento, 2021).

Assim, observa-se que, na trajetória da administração pública, as suas condições políticas, econômicas e sociais são expressas pela precariedade organizacional dos arquivos públicos e o uso incipiente da informação governamental, bem como pelas vulnerabilidades que ocorrem devido às deficiências no processamento técnico, resultado da ausência de padrões de gerenciamento da informação, somada às limitações de recursos humanos, materiais e tecnológicos nos arquivos públicos ou nos serviços arquivísticos dos órgãos governamentais (Jardim, 1996).

Dessa forma, para melhor entendimento, a política nacional de arquivos públicos e privados é definida pelo Conselho Nacional de Arquivos, o qual, como órgão central de um Sistema Nacional de Arquivos tem a finalidade de exercer orientação normativa visando à gestão documental e a proteção especial aos documentos de arquivos (CONARQ, 2020), sendo necessária a prática de ações para a conscientização e sensibilização das organizações quanto à questão da preservação dos documentos digitais, haja vista que as instituições são desprovidas de respaldo para promoverem a preservação desses documentos (Lopes, 2008 *apud* Schäfer & Constante, 2013).

Apesar do avanço do conhecimento arquivístico nos últimos anos, para que se possa alimentar a formulação, implementação e a avaliação de políticas públicas é necessário a ampliação desse conhecimento diante de sua diversidade, desigualdade e à escassez de fontes de conhecimento que possam direcionar essas iniciativas (Jardim, 2009).

Dessa forma, é necessária a persecução de um objetivo prioritário por parte das instituições arquivísticas para que estas possam adquirir mais conhecimentos sobre os objetivos das políticas arquivísticas, não bastando somente uma gestão documental que, de forma clássica, promova o acesso, preservação e a guarda dos documentos, pois, percebe-se uma deficiência na disseminação da informação arquivística por parte dos arquivos públicos brasileiros, apesar de ser o berço de grande parte desses conhecimentos devido a sua atuação e por meio de suas práticas, as quais, na maioria das vezes, são desprovidas de publicidade (Jardim, 2009).

Por fim, pode-se afirmar que diante da missão desafiadora de gerenciar e preservar as informações digitais, é preciso que haja a associação entre a gestão de documentos da instituição com a implantação e o desenvolvimento de políticas, levando em consideração que estas se fazem imprescindíveis para a preservação e acesso dos documentos digitais ao longo do tempo (Schäfer & Constante, 2013).

2.3.1 Técnicas utilizadas na preservação da informação arquivística digital

Em um contexto histórico sobre a preservação digital, observa-se que o seu surgimento aconteceu durante a década de 90 do século XX, ganhando relevância na primeira década do século XXI, diante das exigências de um "desafio digital" (Oliveira, 2014), assim, a partir desse avanço tecnológico, e para que as informações em meio digital sejam preservadas, os profissionais dos arquivos deverão conhecer conceitos e técnicas da tecnologia, considerando que essa intervenção modifica a sua forma de trabalho, sendo necessária à adequação ao novo contexto (Schäfer & Constante, 2013).

Acredita-se que o tempo de vida dos equipamentos eletroeletrônicos é um fator determinante, onde tais equipamentos são normalmente descartados em virtude das inovações tecnológicas, obsolescência acelerada, falhas no funcionamento e custos elevados de reparação, bem como com a implementação de estratégias associadas à obsolescência programada, que modificam a durabilidade dos produtos e os deixam altamente perecíveis, favorecendo, assim, o comportamento consumista (Santos; Guarnieri & Streit, 2021).

Dessa forma, a preservação digital se dá com garantia de que a informação digital permaneça acessível, interpretável e autêntica, mesmo diante de outra plataforma tecnológica daquela que fora inicialmente utilizada no momento da sua criação (Oliveira, 2014), assim, destacam-se as estratégias que se constituem em um conjunto de ações e procedimentos que compõem a manutenção em meio digital, estando estas agrupadas em três classes

fundamentais, sendo elas: migração, emulação e encapsulamento (Schäfer & Constante, 2013).

Nesse sentido, por não durarem para sempre, e ficarem suscetíveis à obsolescência tecnológica, à fragilidade e à perda de confiabilidade, bem como para que as informações estejam acessíveis ao longo do tempo, a migração dos suportes e os formatos aparecem em forma de procedimento de transferência do objeto digital para um suporte ou plataforma de geração tecnológica subsequente, podendo abranger hardware, software e formatos (Innarelli, 2007 apud Schäfer; Constante, 2013), confirmando sua funcionalidade como atividade especifica de preservação, sendo considerada como uma estratégia de longo prazo (Oliveira, 2014).

Já a estratégia de emulação é capaz de superar a obsolescência de software e hardware através de tecnologia que imita sistemas obsoletos em gerações futuras de computador, haja vista que essa técnica se baseia na utilização de um software (denominado emulador) que tem a função de reproduzir o comportamento de um determinado hardware e/ou software em uma plataforma com a qual não era compatível (Cunha & Lima, 2007 apud Schäfer & Constante, 2013), assim se apresenta também como estratégia de longo prazo, confirmando sua funcionalidade como atividade especifica de preservação (Oliveira, 2014).

Quanto à estratégia de encapsulamento trata-se de preservar juntamente com o objeto digital toda a informação necessária e suficiente para suportar o futuro desenvolvimento de conversores, visualizadores e emuladores, ou seja, visa à preservação conjunta do objeto digital, com as informações necessárias ao futuro desenvolvimento de funcionalidades para sua conversão e visualização (Ferreira, 2009 apud Schäfer & Constante, 2013), ratifica-se essa ideia ao afirmar que se trata de um agrupamento de recurso digital e outras coisas mais que se fizerem necessárias para se manter o acesso da informação, podendo ser estruturada por metainformação, visualizadores de software e arquivos discretos que formam o recurso digital (Oliveira, 2014).

2.3.2 Repositório digital confiável de documentos arquivísticos: conceito e principais requisitos

Para que a preservação digital possa acontecer de modo efetivo é preciso se concentrar em ações com resultados em longo prazo e em infraestruturas técnicas e sociais que assegurem a perenidade dos documentos digitais, deixando de focar em ações imediatas, como a preservação dos suportes (Oliveira, 2014).

A Resolução nº 38, do Conselho Nacional de Arquivos, em seu Art. 1º, recomenda aos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR, a adoção das diretrizes publicadas no âmbito do Projeto *The International Research on Permanent Authentic Records in Electronic Systems InterPARES*, da Universidade de British Columbia, Canadá, visando o aperfeiçoamento da gestão e preservação dos documentos de arquivo em formato digital (CONARQ, 2020).

Com a intenção de garantir o controle no ciclo de vida dos documentos arquivísticos digitais, o cumprimento da destinação prevista e a manutenção da autenticidade e da relação orgânica destes documentos, em suas fases corrente e intermediária, faz-se necessário, de preferência, que sejam gerenciados por meio de um Sistema Informatizado de Gestão Arquivística de Documentos – SIGAD, e ainda, que se atente aos cuidados a serem tomados de acordo com um plano de preservação digital, a fim de garantir a referida autenticidade e o acesso dos documentos que serão mantidos por médio e longo prazos (CONARQ, 2022).

O CONARQ apresenta diretrizes de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq, pois se acredita que os arquivos devem dispor de repositórios digitais confiáveis para a gestão, a preservação e o acesso de documentos digitais, nas fases corrente, intermediária e permanente, como solução para a garantia da autenticidade, da preservação e do acesso de longo prazo, haja vista se tratar de uma questão complexa que envolve muitas variáveis, compromissos de longa duração e a necessidade de expressivos investimentos em infraestrutura tecnológica, pesquisa e recursos humanos (CONARQ, 2022).

Neste contexto, afirma-se que um repositório digital para documentos arquivísticos deve ter a capacidade de organizar e recuperar os documentos de forma a manter a relação orgânica entre eles, assim para que se cumpram os requisitos tecnológicos e os procedimentos do tratamento arquivístico, a responsabilidade pelo projeto, implantação e manutenção de um repositório digital de documentos arquivísticos deve ser compartilhada por profissionais de arquivo e de tecnologia da informação (CONARQ, 2020).

Percebe-se, ainda, que a partir de um plano de classificação de documentos, o repositório digital para documentos arquivísticos tem o dever de apoiar a organização hierárquica dos documentos digitais, bem como sua descrição multinível, de acordo com as normas para descrição arquivística: Norma Geral Internacional de Descrição Arquivística – ISAD(G) e Norma Brasileira de Descrição Arquivística – NOBRADE (CONARQ, 2020).

Nesse contexto, para que haja documentos arquivísticos autênticos é preciso que se promova a preservação digital orientada por princípios capazes de gerar efetividade em sua aplicação, os quais são apresentados no quadro abaixo:

PRINCÍPIOS	
• focar especificamente em documentos arquivísticos, e não em objetos digitais de forma genérica; • focar em documentos arquivísticos digitais autênticos; • pressupor que a autenticidade dos documentos arquivísticos digitais está sob ameaça, principalmente no momento da transmissão no espaço (entre pessoas e sistemas) e no tempo (atualização/substituição de hardware e software usados para armazenar, processar e comunicar os documentos); • reconhecer que a preservação digital é um processo contínuo, que começa na concepção do documento; • reconhecer que a autenticidade dos documentos arquivísticos digitais tem por base os procedimentos de gestão e preservação e a confiança tanto no repositório como no órgão responsável pela guarda desses documentos; • arbitrar o que se considera como documento original, uma vez que a preservação digital implica a necessidade de conversão de formatos e atualização de suportes;	• reconhecer que a elaboração de manuais e os procedimentos de preservação desempenhados pelo repositório digital apoiam a presunção de autenticidade desses documentos; • reconhecer que o registro, em metadados, das intervenções de preservação em cada documento apoia a presunção de autenticidade desses documentos; • reconhecer que a autenticidade dos documentos digitais deve ser avaliada e presumida no momento de sua submissão ao repositório. • reconhecer que o repositório digital é responsável pela manutenção permanente da autenticidade dos documentos a ele submetidos; • distinguir claramente a autenticidade e autenticação de documentos, considerando que a primeira é a qualidade de o documento ser verdadeiro, e a segunda é uma declaração dessa qualidade, feita, em um dado momento, por uma pessoa autorizada para tal.

Quadro 1. Princípios de preservação digital
Fonte: Elaborado pelos autores - adaptado para Quadro (CONARQ, 2020).

Por fim, no que se refere ao conceito de independência dos repositórios, isso significa dizer que seu funcionamento e o acesso aos documentos serão independentes das aplicações de funcionamento conjuntas ao mesmo. Cabe ressaltar que os documentos arquivísticos devem estar em formatos que possibilitem sua interoperabilidade com outros repositórios digitais e sistemas informatizados, e para isso o repositório digital também deverá estar em conformidade com as normas e padrões estabelecidos (CONARQ, 2020).

2.3.3 Incidentes de segurança da informação

Existindo situações em que as informações possam estar sob algum tipo risco, este cenário é considerado como um incidente de segurança, podendo ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou redes de computadores, classificados basicamente em duas categorias: incidentes internos e incidentes externos, onde na primeira categoria se pressupõe que o atacante possua prévio conhecimento da estrutura interna da instituição, já na segunda categoria se caracterizam por originarem-se fora da rede da instituição (Ceron *et al.*, 2009).

Entretanto, outro fator a se considerar é a formação da equipe responsável pelo tratamento dos incidentes - CSIRT (*Computer Security Incident Response Team*), pois seus

integrantes deverão atuar de forma completa para analisar, conter e recuperar os ambientes afetados, haja vista que os incidentes podem ocorrer envolvendo os mais diversos conhecimentos e tecnologias, assim sugere-se que sua formação aconteça de forma multidisciplinar (Martins, 2018), haja vista que a capacidade de resposta a incidentes de segurança da informação, a abrangência da ação da equipe de resposta, e o impacto das suas ações, de forma transversal, são enxergados como fator determinante, sendo assim, a sua implementação necessita do apoio da liderança constituída pela organização, bem como o seu treinamento é considerado fundamental (Neves & Correia, 2015).

Nesse contexto, afirma-se a necessidade da estruturação de resposta de incidente de segurança da informação por meio de um planejamento que promova a redução destes incidentes e que ao mesmo tempo contemplem um pacote de ações que possibilitem respostas rápidas, visando mitigar os impactos causados pelos incidentes, bem como permitir o restabelecimento rápido dos sistemas (Ceron *et al.*, 2009).

Metodologia

Este trabalho foi realizado com a utilização dos métodos de pesquisa bibliográfica e exploratória como procedimentos técnicos, com abordagem qualitativa, relacionados à gestão documental, acesso, tratamento de dados e segurança da informação. Buscou-se, ainda, revisar a legislação aplicada ao tema em estudo, prevista na Lei de Arquivos, Lei de Acesso à Informação (LAI) e Lei Geral de Proteção de Dados Pessoais (LGPD), bem como às diretrizes estabelecidas pelo Conselho Nacional de Arquivos – CONARQ, a fim de se verificar a existência de padrões pré-estabelecidos que disciplinem a temática.

Trabalhou-se também com a utilização de dados secundários e análise de periódicos, e no que se refere ao caso prático, a pesquisa ao portal eletrônico do Tribunal de Contas do Estado de Goiás visando à obtenção de informações relevantes e para demonstrar a aplicabilidade de alguns dos conceitos, métodos e ferramentas trazidas por este estudo.

Análise e Discussão dos Resultados

O Tribunal de Contas do Estado de Goiás – TCE-GO foi escolhido dentre os órgãos e entidades custodiadoras de documentos da administração pública do estado de Goiás, a fim de demonstrar a aplicabilidade de alguns dos conceitos tratados em seções anteriores nesta

pesquisa, onde, por meio da verificação de seu sítio eletrônico, buscou-se examinar como foram estruturados os sistemas que tratam da segurança da informação.

Verificou-se, que esse tribunal possui como objetivo garantir o compromisso com a proteção dos dados que ali trafegam, promovendo melhorias em seu sistema, visando a certificação à norma ISO/IEC *(International Organization for Standardization / International Electrotechnical Commission)* 27001:2013, a qual fornece um modelo de melhores práticas para proteger a confidencialidade, a integridade, a disponibilidade e a autenticidade de dados essenciais ao seu pleno desenvolvimento.

Em relação aos requisitos legais, nota-se que o TCE-GO, conforme os normativos apresentados na Tabela 1, promove diretrizes e normas gerais para gestão da segurança da informação, bem como regulamenta o seu plano de segurança institucional. Observa-se também que por meio das Portarias n.º 346 e 518/2022, esse mesmo tribunal proporciona a designação de seu encarregado pelo tratamento de dados pessoais, e também a implementação de seu manual de segurança da informação no âmbito de seus processos de trabalho, conforme disposto na tabela a seguir:

Título	Descrição
Portaria 518/2022	Manual de Segurança da Informação no âmbito dos processos de trabalho do Tribunal de Contas do Estado de Goiás.
Portaria 346/2022-GPRES	Designa o Encarregado pelo Tratamento de Dados Pessoais do Tribunal de Contas do Estado de Goiás.
Resolução Administrativa 11/2022	Dispõe sobre as diretrizes e normas gerais para Gestão da Segurança da Informação do Tribunal de Contas do Estado de Goiás.
Resolução Normativa 08/2022	Regulamenta no âmbito do Tribunal de Contas do Estado de Goiás o Plano de Segurança Institucional.

Tabela 1. Requisitos legais
Fonte: Tribunal de Contas do Estado de Goiás.

Desse modo, após análise da Resolução Administrativa 11/2022, percebe-se que no art. 3º, II, dentre os objetivos constituídos, está o objetivo de instituir diretrizes e normas gerais para o estabelecimento de controles e procedimentos no TCE-GO que assegurem a preservação da informação quanto a sua integridade, confidencialidade, disponibilidade e autenticidade (TCE-GO, 2022).

Assim, após a verificação da Tabela 2, é possível confirmar a instituição de um comitê de segurança da informação de natureza consultiva e deliberativa, com a função de avaliação de documentos sigilosos, responsável por coordenar o sistema de segurança da informação, e por fim, temos, ainda, a normatização da classificação dos ativos de informação produzida no âmbito dos processos de trabalho (TCE-GO, 2022).

Documento	Descrição
Resolução Normativa nº 10/2017	Dispõe sobre os **critérios para promover a classificação das informações confidenciais** produzidas ou custodiadas pelo Tribunal de Contas do Estado de Goiás.
Portaria nº 345/2022 - GPRES	**Comitê de Segurança da Informação (CSSI)**, que exerce a função de Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS.
Portaria nº 376/2022 – GPRES	**Rol de documentos classificados por grau de sigilo** - Classifica os ativos de informação produzidos no âmbito dos processos de trabalho do TCE-GO.

Tabela 2. Classificação da informação
Fonte: Tribunal de Contas do Estado de Goiás.

Pôde-se trazer ao estudo alguns dos processos de tratamento de dados realizados pelo TCE-GO, conforme descrição em seu Manual de Segurança da Informação, referenciado na Tabela 1, o qual tem como objetivo de instituir diretrizes, responsabilidades e normas específicas de segurança da informação, em consonância com a Resolução Administrativa nº 11/2022, que estabeleceu a Política de Segurança da Informação do TCE-GO.

Ressalta-se que as normas ali dispostas devem ser observadas e cumpridas por todos os proprietários, gestores e usuários de informações que trafegam na organização, com vistas à garantida da disponibilidade, integridade, confidencialidade e autenticidade dessas informações.

No que se refere ao controle de acesso das informações no TCE-GO, esse acessos somente serão permitidos mediante identificação e autenticação de usuários, que terão acesso restrito ao que lhes é autorizado e de acordo com perfis de acesso que são pessoais e intransferíveis, sendo estes acessos registrados e sujeitos à rastreabilidade, visando à identificação de acessos que violem as diretrizes e políticas técnicas correlatas.

Quanto à segurança física do ambiente, as instalações do TCE-GO são protegidas conforme o valor dos ativos que estão em seu interior, onde somente o pessoal autorizado e identificado pode permanecer dentro de suas dependências, podendo assim negar acesso a qualquer um que não queira se submeter ao procedimento de identificação. Dessa forma seus colaboradores deverão responder por todo e qualquer acesso aos ativos daquele tribunal, sob sua responsabilidade, assim como pelos efeitos desses acessos efetivados, através de seu consentimento voluntário ou negligente.

No quesito transmissão, TCE-GO determina que é expressamente proibido a transmissão de informação que implique violação de quaisquer leis ou constitua incitamento de qualquer crime, bem como promover a divulgação de qualquer informação restrita ou confidencial sem a permissão de seu proprietário ou do Gestor do recurso ao qual a informação

pertence, para tanto recomenda o compartilhamento de arquivos ou diretórios somente através de meios tecnológicos autorizados pela Gerência de TI. (Ex.: vpn, nuvem privada, diretório na rede).

Quanto ao controle da informação, o Tribunal de Contas do Estado de Goiás, objetivando aplicar medidas preventivas de proteção, detecção e correção corporativamente, para resguardar o ambiente tecnológico determina a proibição de softwares não autorizados por parte da área de tecnologia da informação do TCE-GO.

Ainda, determina que seus sistemas de proteção, como antivírus e firewall, estejam instalados e se mantenham em funcionamento adequado, contando com a aplicação de acessos restritos e o registro de tentativas de acesso a websites maliciosos ou suspeitos, por parte dos usuários.

Neste contexto, os arquivos recebidos por meio de redes, em qualquer mídia de armazenamento, correio eletrônico, arquivos baixados (download) ou em páginas web, devem ser verificados automaticamente quanto à presença de códigos maliciosos, antes de serem utilizados, bem como são realizadas ações para promover o isolamento, ao máximo possível, de ambientes sigilosos do TCE-GO que possam ser contaminados por malwares para evitar impactos de grande magnitude às atividades do negócio, onde são configuradas varreduras automáticas e completas, realizadas regularmente por soluções de antivírus.

Visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação, tendo como objetivo estabelecer diretrizes para o processo de cópia e armazenamento dos dados, todo e qualquer ativo que armazene dados e que esteja sob responsabilidade da Gerência de TI deverá ser considerado para avaliação de inclusão no processo de backup, tendo como prioridade, dentre outras, o conteúdo de repositórios de dados associados a sistemas e os arquivos institucionais de usuários (documentos e e-mails).

Ressalta-se ainda que a Resolução Normativa nº 010/2017, referenciada na Tabela 2, dispõe sobre os critérios para promover a classificação das informações confidenciais produzidas ou custodiadas pelo TCE-GO, além de outros critérios, trata da classificação da informação quanto ao grau de confidencialidade e aos prazos de restrição de acesso, bem como aborda os procedimentos de classificação, reclassificação e desclassificação da informação.

Considerações Finais

Percebe-se na primeira seção, após uma análise conceitual e histórica dos arquivos públicos, por meio da Lei de Arquivos, Lei de Acesso à Informação e da Lei Geral de Proteção de Dados, que essas leis trouxeram conhecimentos atualizados das funcionalidades e da base legal que envolvem o tema em estudo, haja vista a necessidade da observação de seus princípios norteadores, os quais visam à garantia dos direitos individuais, e estabelecem hipóteses que autorizam o tratamento de dados.

Quanto ao tratamento de dados, exposto na segunda seção, entende-se que é preciso desenvolver procedimentos que garantam a gestão dos documentos, bem como a sua preservação e acesso ao longo do tempo, haja vista que as instituições utilizam-se da informação arquivística digital para promoção de suas atribuições.

Ademais, na terceira e última seção, onde se discute a respeito da preservação e segurança da informação arquivística digital, conclui-se que esta preservação deve acontecer em decorrência das vulnerabilidades que ocorrem no meio digital, dentre elas a rápida degradação física dos suportes, a obsolescência tecnológica, a complexidade e os custos de operação, sendo necessário reconhecer que a preservação digital é um processo contínuo, que começa na concepção do documento, e que a autenticidade dos documentos arquivísticos digitais tem por base os procedimentos de gestão e preservação e a confiança tanto no repositório como no órgão responsável pela guarda desses documentos, para tanto o que se propõe é a utilização de repositórios arquivísticos confiáveis, bem como a implementação de procedimentos de gerenciamento dos arquivos.

Conclui-se, que a existência de procedimentos que promovam a preservação da informação arquivística digital é confirmada pela base teórica apresentada nesta pesquisa, haja vista que as formas de enfrentamento desses problemas como a obsolescência tecnológica e os incidentes de segurança da informação já estão sendo desenvolvidos e utilizados pela administração pública conforme foi demonstrado no caso prático deste estudo, onde o Tribunal de Contas do Estado de Goiás, quando regulamenta seu plano de segurança institucional, bem como estabelece diretrizes e normas gerais para gestão da segurança da informação, confirma a aplicabilidade de alguns dos conceitos e métodos tratados neste estudo.

Por fim, espera-se que este estudo possa provocar o desejo em outros pesquisadores a desenvolverem seus trabalhos na busca de técnicas de preservação e segurança da informação

arquivística digital, haja vista sua contemporaneidade e sua importância para todos os órgãos e entidades custodiadoras de documentos da administração pública.

Referências

Belloto, H. L. (2002). Como fazer análise diplomática e análise tipológica de documento de arquivo. São Paulo: Arquivo do Estado. Recuperado em 25 de agosto, 2022, de https://repositorio.usp.br/item/001624887

Botelho, M. C., & Camargo, E. P. do A. (2021). O tratamento de dados pessoais pelo poder público na LGPD. *Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)*, *9*(3), 549–580. Recuperado em 25 de agosto, 2022, de https://portal.unifafibe.com.br/revista/index.php/direitos-sociais-politicas-pub/article/view/1034

Brasil. (2020). Constituição da República Federativa do Brasil de 1988. Recuperado em 08 de agosto, 2022, de http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

Brasil. (2022). Decreto nº 10.474, de 26 de agosto de 2020. Recuperado em 08 de agosto, 2022, de https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm

Brasil. (2022). Lei nº 8.159, de 08 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados. Recuperado em 08 de agosto, 2022, de http://www.planalto.gov.br/ccivil_03/Leis/L8159.htm

Brasil. (2020). Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Recuperado em 08 de agosto, 2022, de http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm

Brasil. (2019). Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações. Recuperado em 08 de agosto, 2022, de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Recuperado em 08 de agosto, 2022, de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brasil (2022). Sobre a Lei de Acesso à Informação - LAI. Ministério Da Justiça e Segurança Pública. Recuperado em 08 de agosto, 2022, de https://www.justica.gov.br/Acesso

Candido, J. P. S., Araújo, T. F. de., & Ribeiro, W. A. C. (2021). Histórico da lei geral de proteção de dados (LGPD). Recuperado em 08 de agosto, 2022, de https://www.advocatta.org/post-ch2sf/historico-da-lei-geral-de-protecao-de-dados-lgpd.

Carvalho de Sá, B., Dutra de Souza, E. H., Reis, L. P., & De Souza Dutra, M. D. (2022). Supply chain network design: a case study of the regional facilities analysis for a 3D printing company. *International Journal of Production Management and Engineering*, 10(2), 211–223. https://doi.org/10.4995/ijpme.2022.17620

Ceron, J. M., Boos Junior, A., Machado, C. S., Martins, F. L. M., & Rey L. F. (2009). O processo de tratamento de incidentes de segurança da UFRGS. Recuperado em 25 de agosto, 2022, de https://lume.ufrgs.br/handle/10183/16096

CONARQ. (2020). Glossário dos documentos arquivísticos digitais. Conselho Nacional de Arquivos. Recuperado em 08 de agosto, 2022, de https://www.gov.br/conarq/pt-

br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glossario-da-ctde

CONARQ. (2020). Resolução nº 23, de 16 de junho de 2006. Conselho Nacional de Arquivos; Dispõe sobre a adoção do Dicionário Brasileiro de Terminologia Arquivística pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR. Recuperado em 22 de novembro, 2022, de https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-23-de-16-de-junho-de-2006

CONARQ. (2020). Resolução nº 27, de 16 de junho de 2008. Conselho Nacional de Arquivos. Recuperado em 25 de agosto, 2022, de https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-27-de-16-de-junho-de-2008

CONARQ. (2020). Resolução nº 38, de 9 de julho de 2013. Conselho Nacional de Arquivos. Recuperado em 25 de agosto, 2022, de https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-38-de-9-de-julho-de-2013

CONARQ. (2022). Resolução nº 43, de 4 de setembro de 2015. Conselho Nacional de Arquivos. Recuperado em 26 de novembro, 2022, de https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-43-de-04-de-setembro-de-2015

Condeixa, F. (2012). Comentários à lei de acesso à informação. *Revista Jus Navigandi*. Recuperado em 25 de agosto, 2022, de https://jus.com.br/artigos/21436. Acesso em: 25 ago. 2022.

de Assis, R. F., de Santa-Eulalia, L. A., Ferreira, W. D. P., Armellini, F., Anholon, R., Rampasso, I. S., & Santos, J. G. C. L. D. (2021). Translating value stream maps into system dynamics models: a practical framework. *The International Journal of Advanced* Manufacturing Technology, 114(11), 3537-3550. https://doi.org/10.1007/s00170-021-07053-y

de Souza Dutra, M. F. Anjos and S. L. Digabel. (2019). A Framework for Peak Shaving Through the Coordination of Smart Homes. 2019 *IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America)*, pp. 1-6, https://doi.org/10.1109/ISGT-LA.2019.8895476

Hora, S. R. A., Saturnino, L. P. T., & Santos, E. C. (2010). A evolução do arquivo e da arquivologia na perspectiva da história. Recuperado em 08 de agosto, 2022, de https://www.webartigos.com/artigos/a-evolucao-do-arquivo-e-da-arquivologia-na-perspectiva-da-Historia/33326/

Jardim, J. M. (1996). A invenção da memória nos arquivos públicos. *Ciência Da Informação*, 25(2), 209-216. https://doi.org/10.18225/ci.inf..v25i2.659

Jardim, J. M. (2009). Diversidade arquivística e políticas de arquivos. *Ponto de Acesso*, *3*(1), 46. https://doi.org/10.9771/1981-6766rpa.v3i1.3312

Jardim, J. M. (2018). Governança arquivística: um território a ser explorado. Revista do Arquivo. Recuperado em 08 de agosto, 2022, de http://www.arquivoestado.sp.gov.br/revista_do_arquivo/07/dossie.php

Júnior, W. de M. C., Real, L. B., Ferreira, A. M. S., & Dutra, M. D. de S. (2022). As ferramentas de qualidade e o Business Intelligence (BI) aplicados à visualização de dados em sistemas informatizados: um estudo de caso. Produto & Produção, 23(2), 101–120. https://doi.org/10.22456/1983-8026.121906

Martins, D. T. (2018). A importância da resposta de incidentes de si. *IMasters - we are developers.* Recuperado em 08 de agosto, 2022, de https://imasters.com.br/devsecops/importancia-da-resposta-de-incidentes-de-si

Nascimento, H. J. C. A. (2021). Políticas públicas para preservação digital: um panorama das inter-relações conceituais da legislação brasileira. Repositorio.ufpe.br. Recuperado em 25 de agosto, 2022, de https://repositorio.ufpe.br/handle/123456789/41086

Neves, P. J. B., & Correia, F. J. R. (2016). Resposta a incidentes de segurança da informação: uma abordagem DOTMLPI-I. *Cyberlaw*, nº 01. Recuperado em 25 de agosto, 2022, de http://hdl.handle.net/10400.26/18023

Oliveira, H. A. (2014). FAUP - A preservação da informação: um contributo para a implementação de um arquivo digital certificável no município do Porto. Retrieved from https://sigarra.up.pt/faup/pt/pub_geral.pub_view?pi_pub_base_id=31766

Prestes, B. R. (2016). Administração pública, um breve histórico. Jusbrasil. Recuperado em 08 de agosto, 2022, de https://bibianarp.jusbrasil.com.br/artigos/304019927/administracao-publica-um-breve-historico

Santos, R. H. M., Guarnieri, P. S., & Streit, J. A. C. (2021). Obsolescência programada e percebida: um levantamento sobre a percepção do ciclo de vida com usuários de aparelhos celulares. *Gestão & Planejamento*, 22, 69–86. https://doi.org/10.53706/gep.v.21.5886

Schäfer, M. B., & Constante, S. E. (2013). Políticas e estratégias para a preservação da informação digital. *Ponto de Acesso*, *6*(3), 108-140. https://doi.org/10.9771/1981-6766rpa.v6i3.6449

Schwaitzer, L. de B. da S. (2019). Instituições públicas e profissionais de arquivo : uma reflexão necessária. *Revista do Arquivo - São Paulo*, 10–12. Recuperado em 25 de agosto, 2022, de http://www.arquivoestado.sp.gov.br/revista_do_arquivo/09/index.php

SERPRO. (n.d.). Princípios da LGPD. Recuperado em 08 de agosto, 2022, de https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/principios-da-lgpd

Tavares, D. W. da S., & Meira Mota, M. (2020). Revisitando a história dos arquivos. *Archeion Online*, *8*(1), 55–67. https://doi.org/10.22478/ufpb.2318-6186.2020v8n1.54771

Tribunal de Contas do Estado de Goiás. (n.d). Classificação da informação - Tribunal de Contas do Estado de Goiás. Recuperado em 29 de agosto, 2022, de https://portal.tce.go.gov.br/requisitos-legais

Tribunal de Contas do Estado de Goiás. (n.d). Requisitos legais - Tribunal de Contas do Estado de Goiás. Recuperado em 29 de agosto, 2022, de https://portal.tce.go.gov.br/classificacao-da-informacao

Submetido em: 01.02.2023

Aceito em: 03.03.2023