UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
DEPARTAMENTO DE ARQUIVOLOGIA
CURSO DE GRADUAÇÃO EM ARQUIVOLOGIA

DOUGLAS NASCIMENTO DE SANTANA

A SEGURANÇA DA INFORMAÇÃO E A ATUAÇÃO DO ARQUIVISTA:
Revisão de Literatura e Relato de Experiência

JOÃO PESSOA

2024

DOUGLAS NASCIMENTO DE SANTANA

A SEGURANÇA DA INFORMAÇÃO E A ATUAÇÃO DO ARQUIVISTA: Revisão de Literatura e Relato de Experiência

Trabalho de Conclusão de Curso (Monografia) apresentada ao curso de Graduação em Arquivologia do da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Arquivologia.

Orientadora: Prof. Ma. Gerlane Farias Alves

S232s Santana, Douglas Nascimento de.
A segurança da informação e a atuação do arquivista revisão de literatura e relato de experiência [manuscrito] : revisão de literatura e relato de experiência / Douglas Nascimento de Santana. - 2024.
42 p. : il. colorido.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Arquivologia) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2024.
"Orientação : Profa. Dra. Gerlane Farias Alves, Coordenação do Curso de Arquivologia - CCBSA. "

1. Segurança da informação. 2. Papel do arquivista. 3. Relato de experiência. 4. Tribunal de Justiça da Paraíba. I. Título

21. ed. CDD 025.171

Elaborada por Livaneide da Silva - CRB - CRB15/638 BSC5/UEPB

DOUGLAS NASCIMENTO DE SANTANA

SEGURANÇA DA INFORMAÇÃO E A ATUAÇÃO DO ARQUIVISTA: Revisão de Literatura e Relato de Experiência

Trabalho de Conclusão de Curso (Monografia) apresentada ao curso de Graduação em Arquivologia do da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Arquivologia.

Aprovada em: 27/06/2024.

BANCA EXAMINADORA

Prof. Ma. Gerlane Farias Alves (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Prof. Dr. Welligton da Silva Gomes
Universidade Estadual da Paraíba (UEPB)

Profa. Dr. Rayan Aramis de Brito Feitoza
Universidade Federal da Paraíba (UFPB)

AGRADECIMENTOS

Gostaria de agradecer e dedicar este trabalho de conclusão de curso as seguintes pessoas:

À professora Gerlane Farias Alves, pelas leituras sugeridas ao longo dessa orientação, pela confiança que me fez ter em mim mesmo e pela dedicação sempre que precisei. Suas orientações foram cruciais para o desenvolvimento deste trabalho, e sua paciência e sabedoria foram fontes constantes de inspiração. Agradeço por cada discussão enriquecedora e pela atenção dedicada a cada detalhe, sempre com a intenção de elevar o nível da pesquisa e do meu aprendizado.

Ao meu pai Lamartine, à minha mãe Marilene, aos meus irmãos Lucas, Felipe e Suellen, e à minha sobrinha Sofia. Vocês foram a base de todo o meu esforço, oferecendo amor incondicional e apoio contínuo. Agradeço por acreditarem em mim, mesmo nos momentos de incerteza, e por serem minha motivação constante. Cada conquista alcançada é, também, de vocês, pois sem o suporte familiar, nada disso seria possível.

Aos meus avós, à minha tia Dulcilene, que sem ela eu não teria iniciado o curso em 2019. Sua ajuda foi fundamental, proporcionando-me a oportunidade de seguir meu sonho acadêmico. À toda minha família, pela compreensão por minha ausência nos momentos em família, e por sempre entenderem que meu compromisso com os estudos demandava tempo e dedicação. Agradeço pelo carinho e suporte emocional, essenciais para meu progresso.

À minha namorada, Gabrielle, que esteve comigo desde o início da minha jornada acadêmica, que sempre me apoiou nos momentos oportunos e por todo apoio neste trabalho. Juntos iniciamos o curso e juntos iremos nos formar. Sua presença constante, palavras de incentivo e compreensão foram vitais para que eu pudesse seguir em frente. Você foi minha parceira em cada etapa deste percurso, e sou eternamente grato por seu amor e dedicação. À minha sogra, Luciana, e cunhada, Maria Eduarda, por todo apoio e carinho,

proporcionando-me um ambiente de tranquilidade e incentivo, essenciais para minha concentração e desempenho acadêmico.

Aos professores da UEPB, em especial, Wellington da Silva, que por meio das disciplinas e debates, através da sua orientação no início deste trabalho, contribuiu significativamente para o desenvolvimento desta pesquisa. Suas aulas e conselhos foram fundamentais para a construção do meu conhecimento e para a estruturação deste trabalho. Agradeço por sua disponibilidade e comprometimento em cada etapa do processo.

Aos funcionários da UEPB, Juliana Marques, Danielle Harlene, Liliane Braga, Marta Patrícia e Rafael Melo, pela presteza e atendimento quando foi necessário. Agradeço profundamente por sempre estarem disponíveis e dispostos a ajudar, proporcionando um ambiente acolhedor e eficiente. Suas habilidades e dedicação ao trabalho não passaram despercebidas e fizeram toda a diferença no desenvolvimento deste trabalho. Cada um de vocês contribuiu de maneira significativa, seja através de suporte administrativo, orientação ou simplesmente com palavras de encorajamento, e por isso sou imensamente grato. Por toda contribuição para o meu desenvolvimento acadêmico e pessoal, vocês foram peças chave nesta trajetória.

Aos colegas do Germania Institut, que me ajudaram ao longo desses anos a me encontrar na minha fé, que me ajudaram a alcançar a paz interior. De certa forma, vocês contribuíram para o fortalecimento da minha identidade e para a realização pessoal que me permitiu focar e concluir este trabalho. Agradeço especialmente ao Abner, André Fiebes, André Schürhaus, Bruno, Daniel, Diogo, Henrique, Leonardo e Vinícius, pelo apoio espiritual e pela Firth que compartilhamos.

Por fim, aos amigos que fiz ao longo desses anos, em especial a Stefanny, Érica, Keila, Pedro, Guilherme, Karol, Inalda e Luciana Colaço pelos momentos de risadas e apoio. A camaradagem e os momentos de descontração foram essenciais para aliviar o estresse e manter a motivação alta. Agradeço pelas discussões construtivas, pela colaboração nos estudos e pelo companheirismo que tornaram essa jornada mais leve e prazerosa.

A todos vocês, meu sincero agradecimento. Esta conquista é reflexo do apoio e carinho de cada um que esteve presente de alguma forma nesta caminhada acadêmica.

RESUMO

A segurança da informação é um desafio atual que afeta organizações públicas e privadas, bem como cidadãos, devido ao aumento dos crimes cibernéticos. Desse modo, este trabalho busca analisar a importância da segurança da informação em ambientes digitais e o papel do arquivista no desenvolviemnto de politicas de segurança contribuindo para a proteção eficaz das informações.Trata-se de uma pesquisa bibliográfica de natureza qualitativa e de caracteristica descritiva onde se busca demonstrar a importância do arquivista na adoção de práticas seguras na segurança da informação, destacando a complexidade do campo, a necessidade de colaboração interdisciplinar e a gestão proativa de riscos. Como exemplo prático, trazemos um relato de experiencia realizado através de estágio não obrigatório no Tribunal de Justiça da Paraíba (TJPB) entre os anos de 2022 e 2024 mostrando o uso do RDC-AQR, apresentando os benefícios e desafios enfrentados na implementação desse sistema, além de destacar sua relevância para a gestão eficiente dos documentos arquivísticos no contexto da instituição e o trabalho realizado pelos estagiários e tecnicos para a implantação e uso de uma politica de segurança da informação. Os resultados evidenciaram a relevância do arquivista na proteção da informação em ambientes digitais, sublinhando a necessidade de aprimoramento dos repositórios institucionais e maior colaboração entre instituições e profissionais da área.

Palavras-Chave: segurança da informação; papel do arquivista; relato de experiência. Tribunal de Justiça da Paraíba.

ABSTRACT

Information security is a current challenge that affects public and private organizations, as well as citizens, due to the increase in cybercrimes. Therefore, this work seeks to analyze the importance of information security in digital environments and the role of the archivist in the development of security policies, contributing to the effective protection of information. It seeks to demonstrate the importance of the archivist in adopting safe practices in information security, highlighting the complexity of the field, the need for interdisciplinary collaboration and proactive risk management. As a practical example, we bring an experience report carried out through a non-mandatory internship at the Court of Justice of Paraíba (TJPB) between the years 2022 and 2024 showing the use of the RDC-AQR, presenting the benefits and challenges faced in implementing this system, in addition to highlighting its relevance for the efficient management of archival documents in the context of the institution and the work carried out by interns and technicians for the implementation and use of an information security policy. The results highlighted the relevance of the archivist in protecting information in digital environments, highlighting the need to improve institutional repositories and greater collaboration between institutions and professionals in the field.

Keywords: Information security; role of the archivist; case study. Court of Justice of Paraíba

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AtoM	Associação Brasileira de Normas Técnicas
CIA	Conselho Internacional de Arquivos
CNJ	Conselho Nacional de Justiça
Conarq	Conselho Nacional de Arquivos
ENSI	Estratégia Nacional de Segurança da Informação
e-ARQ	Modelo De Requisitos Para Sistemas Informatizados De Gestão Arquivística De Documentos
FTP	*File Transfer Protocol*
InterPARES	*International Research on Permanent Authentic Records in Electronic Systems*
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
NBR	Norma Brasileira
PNSI	Política Nacional de Segurança da Informação
PSI	Política de Segurança da Informação
RDC-aqr	Repositório Arquivístico Digital Confiável
SCP	*Secure Copy*
SFTP	*SSH File Transfer Protocol*
TJPB	Tribunal de Justiça da Paraíba
WinSCP	*Windows Secure CoPy*

SUMÁRIO

1. INTRODUÇÃO

A segurança da informação emerge como um dos principais desafios contemporâneos, impactando órgãos públicos, empresas e cidadãos. A perda ou o uso indevido de informações confidenciais podem acarretar prejuízos financeiros, danos à reputação, à violações de privacidade e à facilitação de crimes cibernéticos. Esses crimes, definidos por Roque (2005) como “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”, têm aumentado exponencialmente em frequência e sofisticação. Diante desse cenário, a implementação de políticas públicas e de informação se torna essencial para criar um ambiente digital mais seguro.

As políticas públicas de informação, a partir de instrumentos como a Lei Geral de Proteção de Dados (LGPD), a Estratégia Nacional de Segurança da Informação (ENSI) e a Política Nacional de Segurança da Informação (PNSI), desempenham um papel crucial na regulamentação da coleta e uso de dados pessoais, protegendo a privacidade dos cidadãos e definindo diretrizes para a segurança da informação. A elaboração dessas políticas, no entanto, é uma construção coletiva que envolve governos, empresas e sociedade civil, conforme ressalta Sousa (2006), ao afirmar que "Política Pública não é uma construção de Governo, mas sim uma construção coletiva que tem como atores não só o Governo, mas a sociedade como um todo".

No âmbito da preservação e acesso seguro à informação no Brasil, instituições como o Arquivo Nacional e o Conselho Nacional de Arquivos (CONARQ) são fundamentais. O Arquivo Nacional, através de normas e programas de capacitação, e o CONARQ, com iniciativas como o e-ARQ Brasil, contribuem para a gestão eficaz de documentos digitais, assegurando sua autenticidade e integridade. Exemplos internacionais, como o projeto InterPARES, o modelo OAIS, entre outros, também demonstram a importância da colaboração global na criação de padrões e diretrizes para a preservação da informação digital.

Para delinear nossa pesquisa, temos como problemática o seguinte questionamento: **Qual a importância da segurança da informação em**

ambientes digitais e qual o papel do arquivista no desenvolvimento de politicas de segurança que contribuam para a proteção eficaz das informações?

A escolha do tema deste artigo esta direcionada no papel do arquivista na proteção da informação no âmbito digital, o que nos impulsionou a buscar entender melhor como o arquivista pode contribuir para um ambiente digital mais protegido. Academicamente, reconhecemos a relevância do papel dos arquivistas nesse contexto e buscamos ampliar nosso conhecimento sobre o assunto. Socialmente, acreditamos que a conscientização sobre a importância da proteção da informação é essencial para promover uma sociedade mais resiliente em relação à sua privacidade digital.

À vista disso, o objetivo geral deste trabalho é analisar a importância da segurança da informação em ambientes digitais o papel do arquivista no desenvolvimento de politicas de segurança que contribuam para a proteção eficaz das informações.

Para chegar ao nosso objetivo geral, delineamos os seguintes objetivos especificos: Entender o conceito de informação e o trabalho arquivistico; compreender as preocupações que giram em torno da segurança da informação frente aos avanços tecnologicos; exemplicar a busca pela segurança da informação atraves de alguns projetos existentes, como o projeto interpares; e realizar um breve relato de experiência realizado no Tribunal de Justiça da Paraíba (TJPB) para exemplicar a busca pela segurança da informação em ambientes digitais e a atuação do arquivista perante a temática.

A metodologia utilizada neste trabalho é a pesquisa bibliográfica. O desenvolvimento foi construído com base nas contribuições de diferentes autores que abordam aspectos relacionados à proteção da informação na era digital como Campos (2007) Gordon e Loeb (2002) e Sêmola (2003). A natureza desta pesquisa é qualitativa e de cunho descritivo, visto que busca compreender e descrever os fenômenos e processos relacionados à proteção da informação em abinetes digitais e a atuação dos arquivistas na criação de políticas de segurança.

Lembramos que o referido trabalho está organizado do seguinte modo: Após a introdução, no primeiro seção intitulado “O conceito de informação e o trabalho arquivístico” abordamos a definição de informação, seu papel nas

organizações e na sociedade, bem como a importância do trabalho do arquivista na gestão, preservação e acesso à informação.

No segundo seção intitulado “A Segurança da Informação: novas preocupações frente a tecnologia” dissertamos a respeito da segurança da informação, detalhando as estratégias de proteção de dados, os desafios enfrentados em ambientes digitais e a necessidade de políticas robustas de segurança cibernética para garantir a integridade e confidencialidade das informações.

No terceiro seção intitulado “As Políticas Públicas e as Políticas de Informação: a busca pela Segurança da Informação no âmbito digital” abordarmos sobre as políticas públicas e as políticas de informação onde discutimos a importância das políticas públicas na área de arquivística, destacando a necessidade de interdisciplinaridade e a participação da sociedade civil, bem como as estratégias de implementação e avaliação dessas políticas para garantir o acesso sustentável à informação.

Por fim, na última seção trazemos um breve relato de experiência sobre o uso do RDC-AQR no TJPB através de estágio não obrigatório, apresentando os benefícios e desafios enfrentados na implementação desse sistema, além de destacar sua relevância para a gestão eficiente dos documentos arquivísticos no contexto do Tribunal de Justiça da Paraíba. Por ultimo, apresentamos as considerações finais de nosso trabalho.

2 METODOLOGIA

Para atender aos objetivos propostos neste trabalho, foi realizada uma pesquisa bibliográfica. O referencial teórico foi então construído com base nas contribuições de diferentes autores que abordam aspectos relacionados ao conceito da informação como Floridi (2011) e a segurança da informação como Campos (2007) Gordon e Loeb (2002) e Sêmola (2003). Utilizou-se então as bases de dados como: FEBAB (Federação Brasileira de Associações de Bibliotecários, Cientistas de Informação e Instituições), Academia.edu, Revista USP, Marco Civil da Internet, Repositório da Universidade de Brasília, Books.google, Archiviaria (revista acadêmica semestral revisada por pares publicada pela Associação de Arquivistas Canadenses), Emerald Publishing Limited (editora acadêmica de revistas e livros), e operadores booleanos para busca refinada.

Logo, a natureza desta pesquisa é qualitativa, de cunho descritivo visto que busca compreender e descrever os fenômenos e processos relacionados à proteção da informação e a atuação dos arquivistas na criação de políticas de segurança.

Como exemplo prátIco que envolve o tema tratado, foi utilizado um relato de experiência realizado através de estágio não obrigatório no Tribunal de Justiça da Paraíba (TJPB) entre os anos de 2022 e 2024 fornecendo assim uma análise prática e reflexiva sobre a atuação do arquivista na implementação de medidas de segurança da informação em ambientes digitais. Feito através de observação participativa, este relato de experiência caracteriza-se por uma abordagem descritiva e analítica, focando nos desafios e soluções encontradas na prática profissional atraves do uso do RDC-AQR na instituição.

Através dele buscamos mostrar de forma pratica a preocupação e a atuação do arquivista frente à necessidade de medidas de segurança da informação que devem ser adotadas pelas instituições.

3 O CONCEITO DE INFORMAÇÃO E O TRABALHO ARQUIVÍSTICO

A informação é um conceito multifacetado que permeia diversas áreas do conhecimento, sendo fundamental para o funcionamento e desenvolvimento da sociedade contemporânea.

Segundo Floridi (2011), a informação pode ser entendida como “dados processados, que possuem significado e relevância para aqueles que a utilizam”. Nesse sentido, a informação não se limita apenas à transmissão de dados, mas envolve a interpretação e o contexto em que é utilizada, tornando-se uma ferramenta essencial para a tomada de decisões e a construção do conhecimento.

De acordo com a ISO/IEC 27002:2005, a informação é definida como um conjunto de dados que expressa um ponto de vista, enquanto um dado processado é aquele que se transforma em informação. Antes do processamento, os dados não possuem valor intrínseco, mas após serem processados, tornam-se informações que podem contribuir para a geração de conhecimento por parte de uma organização ou indivíduo. Dessa forma, a informação pode ser entendida como o conhecimento resultante da transformação dos dados por meio de processamento.

Os autores Davenport e Prusak (1998) destacam a importância da informação nas organizações, ao afirmarem que “a informação é um ativo estratégico que impulsiona a inovação e a competitividade”. Isto é, ressaltam que a informação não deve ser apenas vista como um recurso, mas como um diferencial que pode influenciar o desempenho e a posição de uma organização.

Essa perspectiva enfatiza a importância de uma gestão eficiente da informação, desde a coleta e análise até a sua utilização estratégica, como um diferencial para o desenvolvimento e crescimento das organizações no mercado.

Quando se trata da informação no contexto da Arquivística, Duranti (1997) ressalta que a informação arquivística possui características únicas, sendo um reflexo das atividades e decisões humanas ao longo do tempo. Para ela, “os documentos arquivísticos são fontes primárias de informação que

preservam a memória e possibilitam a *accountability* nas instituições".

Por isso, os documentos arquivísticos não podem ser vistos apenas como registros estáticos, mas sim reflexos dinâmicos das atividades e escolhas humanas ao longo do tempo. Esses documentos são considerados fontes primárias de informação que fornecem um panorama autêntico e detalhado das ações e processos realizados por indivíduos e instituições.

Além disso, ao preservarem a memória histórica, esses documentos possibilitam a *accountability* nas instituições, ou seja, a capacidade de prestarem contas de suas ações e decisões perante a sociedade e os órgãos responsáveis. Essa perspectiva destaca o papel fundamental dos arquivos na manutenção da transparência, na preservação da história e na promoção da responsabilidade institucional.

Com avanço da tecnologia, os registros deixaram de ser compostos apenas por suportes materiais e passaram a ser utilizados também em meio digital trazendo novas preocupações sobre seu acesso, divulgação, uso e preservação por parte das instituições e dos profissionais da informação como o arquivista.

O novo cenário exigiu deste profissional uma adaptação contínua e significativa no universo digital, envolvendo não apenas a gestão técnica dos documentos eletrônicos, mas também a compreensão das dinâmicas de preservação, acesso e segurança nesse ambiente virtual. O arquivista tende a desempenhar um papel crucial na implementação de políticas de gestão da informação digital, garantindo a integridade, autenticidade e disponibilidade dos registros digitais ao longo do tempo. Além disso, ele precisa estar atento às questões éticas e legais relacionadas à privacidade, direitos autorais e acesso público às informações digitais sob sua responsabilidade. Essa nova relação com os arquivos digitais demanda do arquivista habilidades multidisciplinares, visão estratégica e constante atualização tecnológica para garantir a eficiência e a relevância de seu trabalho na era digital.

4 A SEGURANÇA DA INFORMAÇÃO: PREOCUPAÇÕES FRENTE À TECNOLOGIA

De acordo com a norma NBR ISO/IEC 27002 (ABNT, 2005), a

segurança da informação consiste em salvaguardar a informação contra diversas ameaças, visando assegurar a continuidade das operações empresariais, reduzir riscos e otimizar tanto o retorno dos investimentos quanto as oportunidades de negócio.

Embora as informações estejam se tornando cada vez mais essenciais para o planejamento estratégico das instituições, sejam elas do âmbito público ou privado, põe-se a análise da segurança da informação como um dos pilares mais fundamentais para as instituições. Desta forma, é crucial garantir a segurança dessas informações, pois elas expõem as organizações a vários riscos, tais como: ataques cibernéticos e exposição inadequada dos dados.

Esses riscos não só afetam a operação das instituições, mas também tornam vulnerável a segurança de outras pessoas envolvidas. Conforme aponta Sêmola (2003), a gestão de segurança da informação abrange três aspectos: tecnológico, físico e humano.

Ao falar desses três aspectos, podemos deduzir que:

1. O aspecto tecnológico envolve o uso de tecnologias, como antivírus, *firewalls*, sistemas de detecção de intrusão, *criptografia*, entre outros, para proteger os sistemas de informação contra ataques cibernéticos, vírus, *malwares* e outras ameaças digitais.
2. Aspecto Físico: Refere-se à segurança física dos recursos de informação, como servidores, data *centers*, dispositivos de armazenamento, etc.
3. Aspecto Humano: Este aspecto considera o comportamento e as ações das pessoas dentro da organização em relação à segurança da informação. Isso inclui a conscientização dos funcionários sobre práticas seguras, políticas de uso aceitável, treinamento em segurança da informação, gerenciamento de acesso e privilégios, além de medidas para prevenir ataques internos, como roubo de dados por funcionários ou manipulação maliciosa de informações.

Logo, as políticas de segurança da informação são fundamentais para estabelecer diretrizes claras e eficazes no âmbito das organizações, principalmente no Brasil, onde a proteção das informações tem se mostrado um desafio crescente devido ao aumento das ameaças cibernéticas.

De acordo com Campos (2007), “Atualmente, as Políticas de Segurança da Informação (PSI) são adotadas em grande parte das organizações em todo o mundo, inclusive no Brasil. Mesmo aquelas empresas que ainda não tem uma política efetiva, reconhecem a necessidade de elaborar e implementar uma”. Dessa forma, a política de segurança da informação estabelece os procedimentos para o acesso às informações em todas as suas formas, tanto interna quanto externamente, determinando quais meios serão utilizados para transportar ou ter acesso a essas informações.

Ainda assim, algumas organizações concentram-se apenas na segurança tecnológica, o que em casos mais comuns, priorizam antivírus, firewalls ou algum “banco de dados”, que em alguns casos não são repositório confiáveis, como o exemplo Repositório Arquivístico Digital Confiável (RDC-Arq), negligenciando assim os demais aspectos importantes para a segurança da informação, como àqueles que criaram e implementaram tais políticas.

4.1 O Arquivista e a Arquivologia perante a segurança da informação

Considerando o contexto da segurança da informação aliado ao papel do profissional arquivista, é fundamental destacar que sua atuação vai além da criação de políticas de segurança. O arquivista desempenha um papel ativo na implementação e manutenção dessas políticas, tendo em vista que uma política bem elaborada e seguida por todos os colaboradores, promove um ambiente harmonioso e protege as informações sensíveis das organizações.

A Segurança da Informação é tida como algo que visa proteger as propriedades da informação. Deste modo, ela aborda alguns elementos que também correspondem às regras existentes na Arquivologia para a realização de atividades nas Unidades de Informação pelos arquivistas. Entre eles podemos citar: a confidencialidade, a integridade, a disponibilidade ou acesso, a autenticidade e o não repúdio.

De acordo com o Glossário documentos arquivísticos digitais, a confiabilidade é a

> Credibilidade de um documento arquivístico enquanto uma

> afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere, e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção (CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS DO CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 18).

A integridade corresponde à

> Estado dos documentos que se encontram completos e que não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada. (CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS DO CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 35).

A disponibilidade ou acesso corresponde ao “Direito, oportunidade ou meios de encontrar, recuperar e usar a informação.” (CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS DO CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 9).

A autenticidade corresponde à

> Credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e que está livre de adulteração ou qualquer outro tipo de corrupção. A autenticidade é composta de identidade e integridade (CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS DO CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 12).

O “não repúdio” tem como objetivo

> “[...] assegurar ao destinatário o “não repúdio” do documento digital, uma vez que, a princípio, o emitente é a única pessoa que tem acesso à chave privada que gerou a assinatura” (CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS DO CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 11).

Vale ressaltar que, ao se tratar de segurança da informação, ela não se limita apenas a sistemas de computação ou informações eletrônicas, tendo em vista que isto abrange diferentes formatos e meios de armazenamento. (Gordon; Loeb, 2002; Sêmola, 2003; ABNT, 2006).

Quando se trata do termo “segurança”, tende-se imaginar a respeito de vários cenários, tendo em vista que a ideia que surge primeiro é que, a segurança envolve proteger algo ou alguém de danos, perigos ou ameaças.

Desta forma, ao tratar sobre a segurança da informação, deve-se ter

a mesma consciência, mesmo que a natureza da segurança possa variar em diversos cenários, assim também como as medidas necessárias para garantir a proteção adequada.

Mas afinal, como garantir a proteção adequada das informações existentes nos documentos? Para garantir essa proteção, é necessário implementar um sistema de segurança da informação que se baseie nos princípios da confidencialidade, integridade e disponibilidade (conforme a Norma ABNT NBR ISO/IEC 27002). Assim, a confidencialidade assegurará que apenas pessoas autorizadas possam ter acesso às informações, a integridade protegerá as informações contra modificações, adulterações ou fraudes, e por fim, a confiabilidade garantirá que apenas os usuários autorizados tenham acesso às informações somente quando solicitado**.**

Dispondo-se evitar que ameaças explorem vulnerabilidades nos ativos relacionados à informação, o que causaria prejuízos aos negócios de uma organização, acreditamos que é preciso que sejam implementadas medidas de segurança robustas, tais como políticas de segurança bem definidas, controle de acesso rigoroso, monitoramento contínuo e treinamento adequado para os funcionários.

Desse modo, para garantir a proteção dos ativos relacionados à informação e evitar que ameaças explorem vulnerabilidades, defendemos ser fundamental a implementação de medidas de segurança robustas. Isso inclui o desenvolvimento de políticas de segurança bem definidas, a implementação de um controle de acesso rigoroso, o estabelecimento de um monitoramento contínuo das atividades e a realização de treinamentos adequados para os funcionários, visando fortalecer a segurança da organização e mitigar possíveis prejuízos aos negócios.

4.2 A competência do arquivista como profissional da informação e a certificação da ISO 27001

No ano de 2005, foi publicado pela International Organization for Standardization (Organização Internacional de Normalização) a ISO 27001 que atua na gestão da segurança da Informação, fornecendo às organizações referências e práticas para identificar, analisar e implementar controles de

segurança da informação, o que auxilia no gerenciamento de riscos, protegendo a integridade, confidencialidade e disponibilidade das informações.

Tendo em consideração que no cenário atual, onde as organizações passaram a utilizar gradativamente *softwares* e *hardwares* para produção de informação, a ISO 27001 estabelece ações para prevenir possíveis vulnerabilidades de segurança na organização, sendo algumas delas: a identificação de ativos, avaliação de riscos, implementação de controles de segurança, gerenciamento de incidentes de segurança dentre outras.

É importante ressaltar a aplicação de PSI, pois elas desempenham um papel fundamental na definição de medidas e práticas de segurança. As PSIs são desenvolvidas levando em consideração as necessidades e os requisitos específicos da organização, bem como os regulamentos e padrões aplicáveis ao setor, de forma com que as organizações possam designar uma cultura de segurança da informação, promovendo a conscientização, reduzindo riscos e protegendo os ativos de informacionais.

No entanto, vale salientar que a aplicação de PSIs devem estar conforme os requisitos baseados na norma ABNT 27002 (2013) Além do mais, a aplicação de quaisquer políticas, deve passar por um processo de definição e aprovação pela direção, sendo necessário que a política seja publicada e comunicada com todos os colaboradores internos e partes externas, como ressalta Costa (2009, p. 48):

> A política por definição é um documento de alto nível, e com isso, não deve conter normas ou procedimentos. Ela deve estabelecer regras de alto nível sobre os recursos tecnológicos da organização e o que deve ser feito e por que ser feito, nunca o “como fazer”. Deve-se criar um documento que os usuários assinem, dizendo que leram, entenderam e concorram com a política estabelecida. Esta é uma parte importante do processo.

A importância do profissional arquivista na elaboração dessas políticas é imprescindível, visto que seu papel na criação das PSIs não se limitaria apenas a garantir a autenticidade das ideias para a preservação da informação. Além de dominar as técnicas relacionadas à gestão do ciclo informacional, que envolve a criação, uso, organização e disseminação da informação, o arquivista como profissional da informação, também desempenha um papel crucial como mediador entre as fontes de informação e seus interessados.

O trabalho em conjunto com o profissional arquivista, tem o objetivo de evitar que ocorram incidentes, uma vez que, alguns desses incidentes ocorrem quando não há controle de acesso. Desta forma, o controle de acesso é fundamental, pois desempenha um papel fundamental na preservação de informações, sejam elas confidenciais voltadas às organizações, assim também como pessoais, como ressalta o Instituto dos Arquivos Nacionais/ Torre do Tombo (2002, p. 40):

> organizações têm de poder controlar quem está autorizado a aceder aos documentos de arquivo e em que circunstâncias o acesso é permitido, dado que os documentos podem conter informação pessoal, comercial ou operacionalmente sensível.

Em suma, o arquivista desempenha um papel essencial na garantia da integridade, acessibilidade e conformidade dos registros e documentos relacionados às Políticas de Segurança da Informação. Além disso, ele é responsável por implementar e monitorar práticas de gestão documental que assegurem a autenticidade e a confiabilidade dos dados ao longo de todo o seu ciclo de vida. Dessa forma, o arquivista contribui significativamente para a proteção dos interesses institucionais e a promoção da transparência e responsabilidade organizacional.

5 AS POLÍTICAS PÚBLICAS E AS POLÍTICAS DE INFORMAÇÃO: A BUSCA PELA SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DIGITAL

A segurança da informação é um dos principais desafios enfrentados por órgãos públicos, instituições privadas e até mesmo pelo cidadão em si. A perda ou uso indevido de informações confidenciais podem trazer prejuízos financeiros, danos à reputação, violação da privacidade e facilitar crimes cibernéticos. Além disso, os ataques cibernéticos têm aumentado exponencialmente em frequência e sofisticação, exigindo respostas robustas e bem planejadas.

Mas afinal, o que são crimes cibernéticos? Segundo Roque (2005, p. 25) crimes cibernéticos são “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”. Portanto, crimes cibernéticos são todas as

ações ilegais e culposas cometidas utilizando dispositivos eletrônicos conectados à internet.

Mas como as políticas públicas e de informação podem combater esse tipo de crime? Políticas públicas e de informação podem combater crimes cibernéticos com leis como a LGPD, diretrizes de segurança, controle de acesso, proteções tecnológicas, treinamento contínuo, planos de resposta a incidentes, cooperação internacional e pesquisas de segurança, criando um ambiente digital mais seguro.

Portanto, para enfrentar esses desafios, é crucial implementar políticas públicas eficazes, como a Lei Geral de Proteção de Dados Pessoais (LGPD), que regula a coleta e o uso de dados pessoais para garantir a privacidade dos cidadãos. Outros exemplos incluem a Estratégia Nacional de Segurança da Informação (ENSI), que estabelece diretrizes para proteger informações em nível nacional, e a Política Nacional de Segurança da Informação (PNSI), que promove a segurança em várias áreas através de ações específicas. É fundamental reconhecer que a formulação de políticas públicas é um compromisso coletivo que envolve governos, empresas e cidadãos, conforme destacado por Sousa (2006, p. 2).

5.1 Instituições Responsáveis e Sistemas de Apoio à Segurança da Informação

A preservação e o acesso seguro à informação são essenciais para garantir a transparência, a *accountability* e a memória. Neste contexto, instituições como o Arquivo Nacional e o (CONARQ) desempenham um papel fundamental na implementação de políticas arquivísticas que visam proteger e gerenciar informações de maneira eficaz.

O Arquivo Nacional, como órgão central do Sistema Nacional de Arquivos (SINAR), tem a responsabilidade de implementar políticas arquivísticas no Brasil. Sua missão é garantir a gestão, preservação e disseminação dos documentos de valor permanente para a administração pública e para a sociedade. Para alcançar esse objetivo, o Arquivo Nacional desenvolve normas, orientações e programas de capacitação que visam assegurar a integridade e a acessibilidade das informações.

O CONARQ, por sua vez, é um órgão vinculado ao Arquivo Nacional,

com a função de definir diretrizes para a política nacional de arquivos públicos e privados. Ele atua na formulação e coordenação de políticas públicas arquivísticas, promovendo a articulação entre os diversos arquivos do país e assegurando a implementação de normas e padrões que favoreçam a segurança da informação.

Um exemplo significativo de iniciativa desenvolvida pelo CONARQ é o e-ARQ Brasil, um modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. Este modelo visa estabelecer padrões para a correta gestão e preservação de documentos digitais, promovendo a criação de repositórios confiáveis que atendam aos requisitos de segurança da informação.

O e-ARQ Brasil (CONARQ, 2011) é essencial para orientar arquivistas, profissionais de tecnologia da informação e administração na aquisição, desenvolvimento ou personalização de sistemas que controlem o ciclo de vida dos documentos e garantam sua autenticidade. Desta forma, o e-ARQ Brasil orienta a criação e manutenção de sistemas que permitem a captura, organização, armazenamento, acesso e preservação de documentos digitais, assegurando sua autenticidade, integridade e confiabilidade ao longo do tempo.

Além do e-ARQ Brasil, existem outros sistemas e iniciativas que contribuem para a segurança da informação. Programas como o RDC-Arq (Repositório Digital Confiável Arquivístico), por exemplo, demonstram como as instituições podem implementar soluções tecnológicas para a gestão de documentos digitais. Portanto, o Arquivo Nacional e o CONARQ devem estabelecer uma política abrangente de preservação de documentos arquivísticos digitais. Essa política permitirá que os órgãos públicos implementem programas de gestão documental que assegurem a preservação e o acesso a longo prazo. Ao incluir estratégias para enfrentar a obsolescência tecnológica e definir um local adequado para arquivar documentos digitais e nato-digitais, garantem que as informações permaneçam acessíveis e íntegras, independentemente das mudanças tecnológicas, reforçando a segurança e a confiabilidade da gestação informacional.

As iniciativas desenvolvidas pelo Arquivo Nacional, CONARQ e outras instituições são essenciais para a construção de repositórios confiáveis

e seguros. Um modelo de orientação para a cosntruçaõ de sitemas como o e-ARQ Brasil fortalecem a segurança da informação, estabelecendo padrões e diretrizes que garantem a gestão adequada dos documentos digitais. Essas ações não só preservam a memória institucional, mas também asseguram a transparência e a confiança no manejo das informações, contribuindo para a boa governança e a integridade administrativa.

Elaborar uma PSI envolve uma série de passos fundamentais para garantir a proteção adequada dos dados e informações. Esses passos são essenciais para estabelecer diretrizes claras e eficazes que visam a segurança dos sistemas e dados organizacionais. Para elaborar uma PSI, é importante seguir cinco passos como ilustrado na imagem abaixo:

Figura 1: 5 passos para elaborar uma PSI

Fonte: Elaborado com base no vídeo do canal “Starti” no YouTube.

A imagem ilustrativa dos 5 passos para elaborar uma PSI, baseada no vídeo do Youtube “Políticas De Segurança Da Informação Em 5 Passos” apresentado por Fernando Pisolato em 2016, nos mostra uma abordagem visual clara e concisa sobre as etapas essenciais para a criação de uma Política de Segurança da Informação. Através dessa imagem simplificamos a compreensão dos processos envolvidos, oferecendo um guia visual que facilita a assimilação das informações e a implementação prática das políticas. Abaixo descreveremos cada passo:

1. Planejar: Nesta etapa, são identificadas as necessidades específicas de segurança da informação da organização. Isso

inclui avaliar os ativos críticos, identificar ameaças e vulnerabilidades, e definir objetivos claros para a PSI.

2. Elaborar: Aqui, as diretrizes, normas e procedimentos são desenvolvidos com base nos resultados da etapa de planejamento. Isso envolve criar documentos detalhados que descrevem como os dados e sistemas devem ser protegidos e gerenciados.
3. Documentar: É crucial documentar todas as políticas e procedimentos definidos na fase anterior. Essa documentação deve ser clara, acessível e constantemente revisada e atualizada para refletir mudanças na tecnologia, na organização ou nas ameaças.
4. Aprovar: A PSI deve ser revisada e aprovada pela alta administração da organização. Isso garante que as políticas sejam oficialmente reconhecidas e apoiadas pela liderança, garantindo comprometimento e recursos para implementação.
5. Treinar e Implementar: Por fim, todos os funcionários devem ser treinados sobre as políticas de segurança da informação. Isso inclui conscientização sobre práticas seguras, procedimentos específicos a serem seguidos e a importância da segurança da informação para a organização.

Esses passos são fundamentais para estabelecer uma cultura de segurança da informação robusta e eficaz dentro de qualquer organização.

5.2 O Projeto *InterPARES* e suas contribuições

Desde o seu início em 1999, o projeto *International Research on Permanent Authentic Records on Electronic Systems* (InterPARES) tem sido reconhecido como um marco na área da preservação da informação digital. Concebido por uma equipe internacional de especialistas em Arquivologia e Ciência da Informação. Segundo Indolfo e Lopes (2015), o InterPARES surgiu para

> Desenvolver o conhecimento essencial para a preservação a longo prazo de documentos arquivísticos autênticos, produzidos e/ou mantidos em formato digital, e fornecer as bases para padrões, políticas, estratégias e planos de ação capazes de garantir a longevidade de tais materiais e a capacidade de seus usuários confiarem em sua autenticidade. (Indolfo; Lopes, 2015, p.1)

Desta forma, o projeto InterPARES é uma resposta à necessidade premente de estabelecer padrões e diretrizes que asseguram a autenticidade e a confiabilidade dos registros eletrônicos em um cenário cada vez mais digitalizado e suscetível a ameaças à integridade informacional.

Uma das contribuições mais significativas do InterPARES foi a elaboração de modelos teóricos e práticos para a preservação de documentos digitais autênticos e confiáveis. Esses modelos, resultados de pesquisas aprofundadas e colaborações internacionais, delinearam diretrizes abrangentes para o desenvolvimento de políticas, normas e legislações, visando sua preservação a longo prazo, garantindo não apenas sua acessibilidade contínua, mas também a integridade e autenticidade das informações. Sendo assim:

> Gerar os quadros teóricos e metodológicos para desenvolver políticas, procedimentos, regulamentos, normas e legislação locais, nacionais e internacionais, a fim de garantir a confiança pública baseada em evidências de boa governança, uma economia digital forte e uma memória digital persistente (INTERPARES TRUST, 2020).

O InterPARES exerceu um impacto substancial na segurança da informação em diversas instituições ao redor do mundo. Suas diretrizes para verificação da autenticidade e confiabilidade dos documentos eletrônicos tornaram-se fundamentais para a implementação de políticas de gestão documental que visam mitigar riscos associados à perda de dados e garantir continuidade informacional em ambientes digitais.

Além disso, o projeto InterPARES promoveu uma valiosa colaboração entre países e instituições, propiciando a troca de conhecimentos, experiências e melhores práticas no âmbito da preservação digital. Essa cooperação internacional foi essencial para enfrentar desafios complexos e globais relacionados à preservação informacional.

O projeto InterPARES passou por 4 etapas, desde seu ano de criação em 1999 até o ano de 2021. A primeira etapa do InterPARES (1999-2001), chamada InterPARES 1, abordou a preservação de documentos eletrônicos autênticos e inativos. Participaram equipes de pesquisadores de diversos países, como China, Europa, Itália, Estados Unidos, e uma equipe internacional, todos com um contexto jurídico-administrativo comum (INTERNATIONAL…, 2001, p. 1). Abaixo, ilustramos uma linha do tempo das etapas do Projeto InterPARES.

Figura 2: Etapas do Projeto InterPARES

Fonte: elaborada pelo autor

A segunda etapa do Projeto InterPARES, denominada InterPARES 2 (2002-2006), teve como objetivo desenvolver bases teóricas para a

preservação de documentos de arquivo gerados por sistemas experimentais, interativos e dinâmicos, levando em conta seus processos de criação e usos potenciais nas áreas artística, científica e governamental.

Foram formuladas metodologias para garantir a confiabilidade e autenticidade desses documentos, considerando a coleta de documentos para fins legais, administrativos, sociais e culturais após a conclusão de suas finalidades originais.

> Além disso, a etapa focou na preservação autêntica e a longo prazo dos documentos recolhidos, bem como na análise e avaliação de tecnologias para implementar essas metodologias, respeitando a diversidade cultural e o pluralismo. Com base nos resultados do InterPARES 1, essas metodologias foram aplicadas a novos tipos de sistemas mencionados (INTERNATIONAL…, 2006, p. 1).

Na terceira etapa, os fundamentos teóricos e métodos sobre preservação digital desenvolvidos nas duas fases anteriores foram aplicados em planos de ação concretos para organizações que necessitam de preservação a longo prazo, mas possuem recursos limitados. Os módulos de ensino foram elaborados para abordar como a teoria geral e os métodos podem ser implementados em arquivos e unidades de pequeno e médio porte, identificando os fatores que determinam o tipo de implementação adequada e as habilidades necessárias para os profissionais realizarem essas operações (DURANTI, 2007, p. 579). Com o financiamento do *Canada's Social Sciences and Humanities Research Council's Community – University Research Alliances gran*t, a terceira fase do InterPARES contou com a participação de equipes da África, Brasil, Canadá, Catalunha, China, Colômbia, Coreia, Itália, Malásia, México, Noruega e Turquia. Foram desenvolvidos requisitos para organizações arquivísticas de diversos contextos, públicas e privadas, de pequeno e grande porte, responsáveis pela preservação de documentos digitais autênticos resultantes de atividades governamentais, de negócios, de pesquisa, artísticas, de entretenimento e culturais (Duranti, 2007, p. 586; INTERNATIONAL…, s.d.a).

Na quarta etapa, conhecida como InterPARES Trust ou ITrust, o objetivo foi desenvolver teorias e metodologias para políticas, procedimentos, normas e legislações voltadas a documentos de arquivo digitais produzidos em ambientes acessíveis pela internet, garantindo sua confiabilidade. Para isso,

> foram avaliados os resultados das políticas e práticas atuais sobre tratamento arquivístico de documentos digitais em ambiente online por instituições; refletidas as problemáticas sobre segurança da informação e declínio de confidencialidade devido ao aumento da produção de documentos em ambientes online; estabelecidos modelos de políticas, procedimentos e práticas para criação, gerenciamento, acesso e armazenamento de documentos digitais na internet, com foco em redes sociais, computação em nuvem e tecnologias móveis; e determinadas propostas e modelos com requisitos funcionais para sistemas de armazenamento e gerenciamento desses documentos (Duranti; Jansen, 2013, p. 64-65).

A equipe de pesquisadores do ITrust era composta por organizações e universidades públicas e privadas de caráter internacional e interdisciplinar, inicialmente dividida em cinco grupos principais: América do Norte, Europa, Ásia, América Latina, organizações multinacionais e em 2015 foram adicionados dois novos grupos, sendo eles da Australásia e África.

Atualmente, o legado do projeto InterPARES subsiste como um paradigma exemplar de como a colaboração internacional, aliada a um embasamento teórico consistente e à prática efetiva, pode influenciar significativamente políticas de informação em escala global. Sua contribuição para a segurança, preservação e acessibilidade da informação digital é amplamente reconhecida e continua a orientar e aprimorar práticas arquivísticas e de gestão da informação em diversos contextos institucionais ao redor do mundo.

6 RELATO DE EXPERIÊNCIA: USO DO RDC-Arq NO TRIBUNAL DE JUSTIÇA DA PARAÍBA

O termo Repositório Arquivístico Digital Confiável (RDC-arq) surgiu através da resolução n.º 43 do Conarq, de setembro de 2015, anteriormente denominado Repositórios Digitais Confiáveis de Documentos Arquivísticos pela Resolução n.º 39 de abril de 2014.

Essa mudança de nomenclatura é significativa, pois indica a especificidade de um Repositório Digital Confiável (RDC) com atributos arquivísticos. Além disso, é importante notar que as resoluções n.º 43 e n.º 39 foram revogadas, sendo substituídas pela Resolução n.º 51 de 25 de agosto de

2023, que estabelece novas diretrizes para a gestão de repositórios digitais confiáveis no âmbito arquivístico.

Durante o estágio não obrigatório realizado no Tribunal de Justiça da Paraíba (TJPB), houve a designação do autor para auxiliar na implementação e no uso do RDC-arq, um repositório digital confiável destinado à preservação de documentos arquivísticos eletrônicos.

O TJPB iniciou a adoção do RDC-arq visando modernizar e garantir a preservação e o acesso contínuo a documentos digitais, em conformidade com as normativas do CONARQ.

A transição para o meio digital pretendia não apenas aumentar a eficiência administrativa, mas também assegurar a integridade e a autenticidade dos documentos judiciais. Porém, vale salientar que apesar da facilidade de criação, acesso e compartilhamento, os documentos em ambientes digitais enfrentam vulnerabilidades significativas, como rápida degradação física, obsolescência tecnológica, complexidade e altos custos de preservação a longo prazo (Santos; Flores, 2015). Logo, as fragilidades dos documentos arquivísticos digitais suscitam preocupações significativas acerca da preservação digital, um tema intrincado e oneroso.

No contexto digital, é crucial repensar a garantia da cadeia de custódia ininterrupta, assim como garantir a administração arquivística, preservação duradoura e custódia confiável desses documentos. Essa necessidade é impulsionada pela Lei 8159/91 (BRASIL, 1991), que atribui ao setor público a responsabilidade pela gestão dos documentos de arquivo, visando sua eliminação ou guarda permanente. Entretanto, a implementação do RDC-arq trouxe alguns desafios, um dos principais foi a necessidade de adequação de infraestrutura tecnológica por parte dos servidores, como também dos estagiários, assim como a falta treinamento para o uso do RDC-aqr.

É importante destacar que o RDC-arq foi implementado no TJPB de forma que os estagiários do arquivo do fórum cível ficariam responsáveis pelo seu manuseio e pela instrução dos novos estagiários, sem a orientação adequada dos responsáveis pelo repositório ou o treinamento necessário. Isso resultou em problemáticas, como inconsistências no uso do sistema, retrabalho devido a erros operacionais e uma curva de aprendizado mais lenta, comprometendo a eficiência e a eficácia do processo arquivístico.

Por meio dessa experiência, entendemos na prática a importância da preservação digital e os cuidados necessários para manter a autenticidade e a confiabilidade da informação no âmbito digital. A falta de treinamento adequado continua sendo uma barreira significativa, evidenciando a necessidade urgente de programas de capacitação estruturados para todos os envolvidos.

A experiência no estágio no TJPB com o uso do RDC-arq foi extremamente valiosa, tendo em vista a possibilidade de desenvolver habilidades técnicas e um entendimento profundo sobre a gestão de documentos digitais. A adoção do RDC-arq provou ser uma medida eficaz para assegurar a preservação e o acesso seguro a informações judiciais, alinhando-se às melhores práticas arquivísticas contemporâneas.

Apesar dos desafios enfrentados, como a falta de treinamento adequado e a necessidade de ajustes na infraestrutura tecnológica, a experiência reforçou a importância da preservação digital e destacou a necessidade de melhorias contínuas para garantir a eficiência e a eficácia dos processos arquivísticos. Além disso, essa vivência ressaltou o papel crucial do arquivista na elaboração de políticas de informação, assegurando que os sistemas adotados não apenas atendam aos requisitos técnicos, mas também promovam a integridade, a acessibilidade e a confiabilidade das informações ao longo do tempo.

Abordando um pouco mais sobre o uso do RDC-arq no Tribunal de Justiça da Paraíba (TJPB), é possível destacar como essa ferramenta revolucionou a gestão de documentos e informações dentro da instituição. As imagens a seguir oferecem uma visão mais concreta e ilustrativa desses avanços, mostrando como o RDC-arq contribuiu para a eficiência operacional, a segurança dos dados e o acesso ágil às informações relevantes.

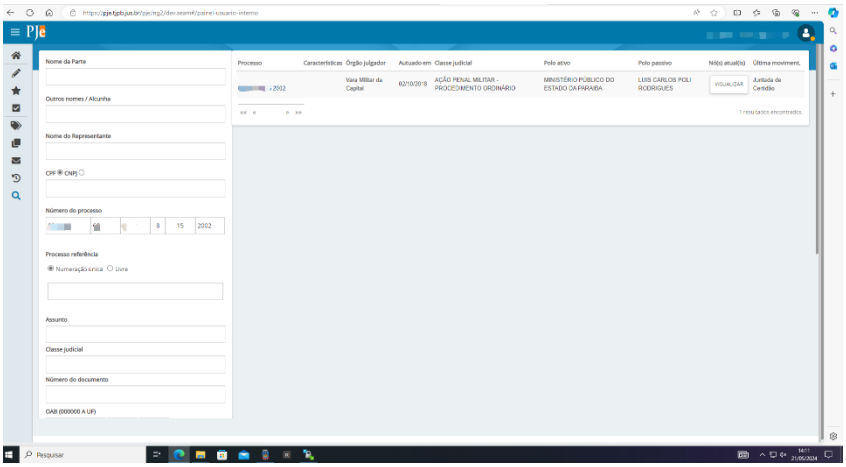
Além disso, ressaltamos a importancia do uso de ferramentas essenciais para a gestão documental no TJPB, como o Archivematica, uma solução para preservação de longo prazo de conteúdos digitais, o AtoM *(Access to Memory)*, um aplicativo de descrição arquivística integralmente voltado para a web e baseado nas normas do Conselho Internacional de Arquivos (CIA), o PJE (Processo Judicial Eletrônico), que é a página do tribunal de Justiça onde temos acesso aos processos eletrônicos e o WinSCP (*Windows Secure CoPy*),

um cliente livre e de código aberto para os protocolos SFTP *(SSH File Transfer Protocol)*, SCP (*Secure Copy*) e FTP (*File Transfer Protocol*)

Inicialmente, acessamos o (Processo Judicial Eletrônico) (PJE) que é utilizado para baixar os processos em formato PDF, permitindo o acesso e a visualização dos documentos. Esses arquivos são então armazenados em pastas específicas. Em seguida, o WinSCP *(Windows Secure CoPy)* é empregado para transferir esses documentos para um servidor seguro, garantindo a integridade e a confidencialidade das informações durante o processo de transferência. Após o armazenamento seguro, entra em cena o Archivematica, que desempenha um papel crucial na preservação de longo prazo dos conteúdos digitais, garantindo sua acessibilidade e autenticidade ao longo do tempo. Por fim, o AtoM *(Access to Memory)* é utilizado para criar a descrição arquivística detalhada de cada processo, permitindo não apenas o acesso às partes do processo, mas também fornecendo informações valiosas sobre sua origem, conteúdo e contexto. Dessa forma, o usuário pode navegar de forma eficiente pelos documentos, entender sua estrutura e obter uma visão completa da informação arquivística

Abaixo temos a tela inicial do PJE que foi desenvolvido pelo Conselho Nacional de Justiça (CNJ), com intuito de informatizar a tramitação dos processos judiciais no Brasil, permitindo que todas as etapas sejam realizadas de forma digital. Seu principal objetivo é modernizar e agilizar o andamento dos processos, proporcionando maior eficiência, transparência e economia de recursos, além de facilitar o acesso à justiça.

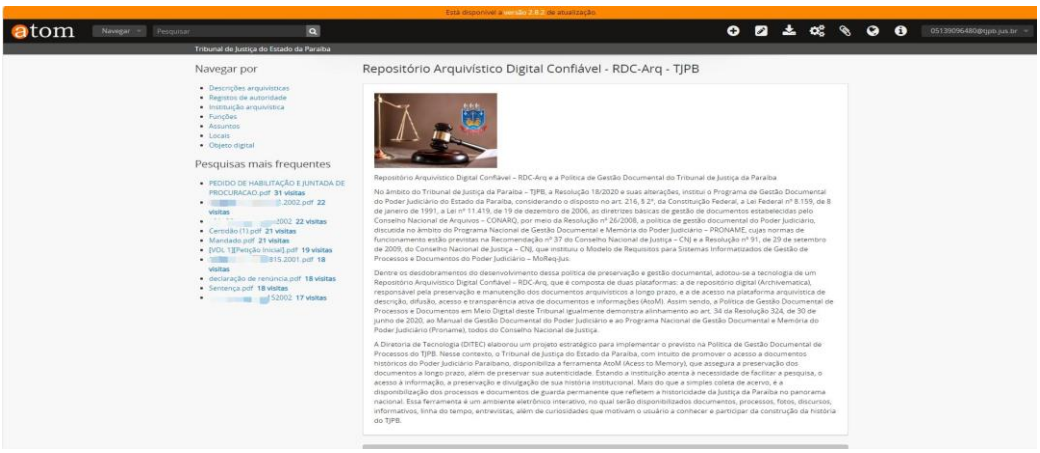
Figura 3: Página do PJE (Processo Judicial eletrônico)



Fonte: TJPB - Processo Judicial Eletrônico

Já na figura abaixo podemos observar a plataforma AtoM (Access to Memory) utilizada pelo TJPB. O AtoM é um sistema de gerenciamento de informações arquivísticas desenvolvido para permitir o acesso e a divulgação de acervos arquivísticos de forma organizada e eficiente. O AtoM é um aplicativo de descrição arquivística integralmente voltado para a web e baseado nas normas do Conselho Internacional de Arquivos (CIA). Ele permite a organização estruturada de informações, metadados e descrições de acervos, tornando mais fácil a localização e a recuperação de documentos pelos usuários interessados, sejam eles pesquisadores, acadêmicos ou cidadãos em geral.

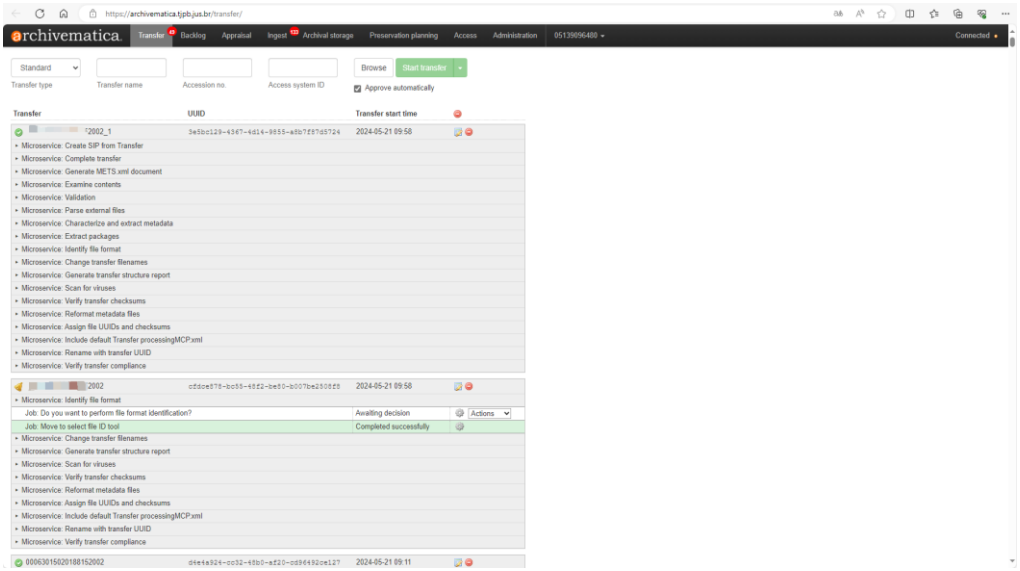
Figura 4: Página do TJPB no AtoM



Fonte: Tribunal de Justiça da Paraíba

Abaixo podemos observar a página do TJPB no Archivematica, que é uma plataforma de preservação digital. O Archivematica é utilizado para gerenciar e preservar arquivos digitais a longo prazo, garantindo a integridade, acessibilidade e autenticidade dos documentos arquivísticos. Ele automatiza processos de preservação, permitindo que os arquivos sejam armazenados e mantidos de acordo com padrões internacionais.

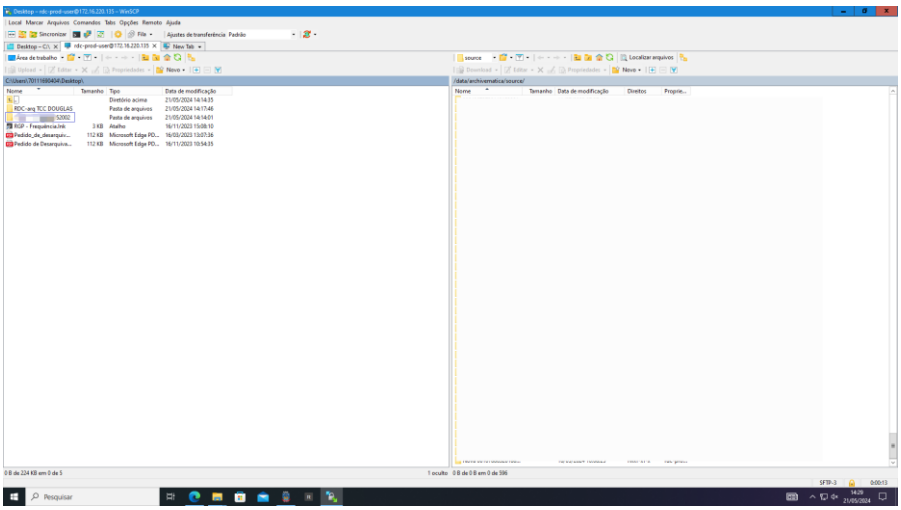
Figura 5: Página do TJPB no Archivematica



Fonte: Tribunal de Justiça da Paraíba

A Figura 5 mostra o software WinSPC, que é utilizado para transferência de arquivos através dos protocolos FTP, SCP, entre outros. É um aplicativo eficiente para manipulação de arquivos via FTP, facilitando a transferência segura e organizada de arquivos entre diferentes sistemas e servidores.

Figura 6: WinSCP (*Windows Secure CoPy*)



Fonte: Tribunal de Justiça da Paraíba

Desse modo, podemos deduzir a importância dos sistemas apresentados para a gestão e preservação de informações no âmbito do Tribunal de Justiça da Paraíba (TJPB). O PJE (Processo Judicial Eletrônico)

moderniza e agiliza a tramitação dos processos judiciais, enquanto o AtoM (Access to Memory) organiza e facilita o acesso a acervos arquivísticos. O software WinSPC oferece uma solução eficiente para a transferência de arquivos via protocolos como FTP e SCP, e o Archivematica assegura a preservação digital a longo prazo dos documentos arquivísticos. Juntos, esses sistemas contribuem significativamente para a eficiência, transparência e segurança na gestão da informação no TJPB.

7 CONSIDERAÇÕES FINAIS

Neste trabalho, foi possível realizar uma análise abrangente sobre o papel do arquivista na segurança da informação em ambientes digitais e sua participação no processo de elaboração de políticas de segurança da informação.

Ao longo das seções, foram explorados diversos aspectos, desde a definição e importância da informação até a implementação de políticas e práticas de segurança assim como exploramos exemplos existentes de políticas de informação e sua implantação. Através da pesquisa bibliográfica e da produção do referencial teórico, alcançamos uma visão ampla e aprofundada do tema, contribuindo assim para o entendimento da importância do arquivista na proteção da informação e na promoção de práticas seguras em ambientes digitais.

A discussão sobre o papel do arquivista na segurança da informação destaca a complexidade crescente desse campo, a necessidade de colaboração interdisciplinar, os desafios atuais, a importância de uma cultura organizacional de segurança e a gestão proativa de riscos para garantir a proteção eficaz dos dados em ambientes digitais.

Neste trabalho, discutimos a importância dos arquivistas na segurança da informação em ambientes digitais, seu envolvimento no desenvolvimento de politicas de segurança e os desafios e oportunidades nesse contexto.

Destacamos o papel crítico da informação nas organizações e na sociedade, ressaltando a relevância do trabalho dos arquivistas na gestão, preservação e acesso à informação para promover a transparência e a responsabilização.

Buscamos analisar as políticas e práticas de proteção de informações em ambientes digitais, enfatizando a necessidade de políticas e procedimentos fortes para garantir a integridade, confidencialidade e disponibilidade dos dados. Identificamos desafios enfrentados pelos arquivistas e oportunidades para desenvolver medidas de segurança mais eficazes.

Abordamos o papel ativo dos arquivistas no desenvolvimento e implementação de políticas de segurança da informação, destacando a importância do conhecimento técnico e da colaboração entre disciplinas. Também discutimos a intersecção entre política pública e política de informação, enfocando a segurança da informação na esfera digital.

Apresentamos um relatório sobre a experiência do TJPB com a RDC-AQR, descrevendo as medidas tomadas para garantir a segurança dos registros arquivísticos digitais. Acreditamos que esse exemplo reforça a importância da implementação de medidas de segurança e destaca a consciência da importância da segurança da informação.

Concluímos que os arquivistas desempenham um papel estratégico na proteção dos ativos de informação e na promoção de um ambiente digital seguro e confiável. Esse trabalho também destaca a relevância contínua dos arquivistas na era digital e a necessidade de estratégias abrangentes para a segurança da informação.

Esperamos ter dado uma contribuição à área de Arquivologia ao explorar tais aspectos e desejamos que nosso trabalho inspire novas pesquisas sobre o assunto auxiliando na disseminação de produções sobre o tema estudado.

Durante a produção deste trabalho, enfrentamos desafios significativos, como a dificuldade de encontrar materiais relevantes em repositórios acadêmicos e bibliotecas digitais. Além disso, a escassez de fontes específicas sobre a interseção entre a arquivologia e a segurança da informação em ambientes digitais limitou o escopo da pesquisa. Para superar essas barreiras, sugerimos a ampliação e o aprimoramento dos repositórios acadêmicos, além de uma maior colaboração entre instituições de ensino e profissionais da área para disponibilizar mais recursos e estudos específicos. Isso contribuiria não apenas para a facilidade de acesso a informações essenciais, mas também para o enriquecimento do campo de estudo, facilitando futuras pesquisas e a

elaboração de políticas de segurança da informação mais robustas e informadas.

REFERÊNCIAS

ABNT. ABNT NBR ISO/IEC 27001. Tecnologias da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT. Rio de Janeiro, 2013, 32 p.

ABNT. ABNT NBR ISO/IEC 27002. Tecnologias da informação – Código de pratica para controles de segurança da informação. ABNT. Rio de Janeiro, 2005, 112 p.

BELLUZZO, R. C. B. As competências do profissional da informação nas organizações contemporâneas. Revista Brasileira de Biblioteconomia e Documentação, [S. l.], v. 7, n. 1, p. 58–73, 2011. Disponível em: https://rbbd.febab.org.br/rbbd/article/view/180. Acesso em: 9 jun. 2024.

BRASIL. Conselho Nacional de Arquivos (CONARQ). Disponível em: https://www.gov.br/conarq/pt-br. Acesso em: 24 mai. 2024.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Política Nacional de Segurança da Informação (PNSI). Disponível em: https://www.gov.br/gsi/pt-br/ssic/politicas-nacionais/politica-nacional-de-seguranca-da-informacao-pnsi. Acesso em: 24 mai. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 mai. 2024.

BRASIL, E. A. R. Q.; BRASIL, A. R. Q. Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. Conselho Nacional de Arquivos, 2011.

CAMPOS, André. Sistema de segurança da informação. Controlando os Riscos, 2007.

CONSELHO NACIONAL DE ARQUIVOS. Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq. Rio de Janeiro: Arquivo Nacional, 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. Glossário de documentos arquivísticos digitais. Versão 8.0. Rio de Janeiro: CONARQ, 2020, 62 p. Disponível em: http://conarq.gov.br/images/ctde/Glossario/glosctde_2020_08_07.pdf. Acesso em: 25 mai. 2024.

DA COSTA, DANIELLE ROCHA. Fatores Críticos de Sucesso para Elaboração de Políticas de Segurança da Informação e Comunicações no Âmbito da Administração Pública Federal. Universidade de Brasília, 2009.

DAVENPORT, T. H., & PRUSAK, L. Working knowledge: How organizations manage what they know. Harvard Business Press, 1998.

DOS SANTOS, Henrique Machado et al. As vulnerabilidades dos documentos digitais: Obsolescência tecnológica e ausência de políticas e práticas de preservação digital. Biblios Journal of Librarianship and Information Science, n. 59, p. 45-54, 2015.

DURANTI, L. Diplomatics: New uses for na old science. Archivaria, 43, 1-19, 1997.

DURANTI, Luciana; PRESTON, R. International research on permanent authentic records in electronic systems, 2008.

FLORIDI, L. The philosophy of information. Oxford University Press, 2011.

GORDON, L. A.; LOEB, M. P. The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), v. 5, n. 4, p. 438-457, 2002.

INDOLFO, Ana Celeste; LOPES, Vera Hess. Entrevista com Luciana Duranti, 2015.

INSTITUTO DOS ARQUIVOS NACIONAIS/TORRE DO TOMBO. Caderno de Recomendações para gestão de documentos de arquivo electrónicos: modelo de requisitos para gestão de arquivos electrónicos (MoReq). Lisboa: [s.n.], 2002. Disponível em: http://www.iantt.pt. Acesso em: 20 de jun. 2023.

JANSEN, Adam; DURANTI, Luciana. The InterPARES Trust Project – Trust and digital records in na increasingly networked society. GILLILAND, Anne; McKEMMISH, Sue; STANCIC, Hrvoje; SELJAN, Sanja, p. 63-68, 2013.

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO EM 5 PASSOS. Direção/Produção: Fernando Pisolato. Local: Starti Soluções em TI, 2016. 1 vídeo (3 min.). Publicado pelo canal Starti. Disponível em: https://youtu.be/nI1o-w4nKdc?si=yBAok3NFz7S5a9wP. Acesso em: 14 de jun. 2024.

SÊMOLA, M. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro: Campus, 2003.

SCHNEIDER, Marilda Pasqual. Dispositivos de accountability na reforma da educação básica brasileira: tendências em curso. Revista Diálogo Educacional, v. 19, n. 60, p. 469-493, 2019.

THE INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (InterPARES). InterPARES Trust. Disponível em: https://interparestrust.org/. Acesso em: 18 mai. 2024.

ANEXO A – AUTORIZAÇÃO PARA A REALIZAÇÃO DA PESQUISA

TERMO DE AUTORIZAÇÃO PARA USO DE IMAGEM PARA A REALIZAÇÃO DO TRABALHO DE CONCLUSÃO DE CURSO

Senhor(a) Chefe,

Solicitamos a autorização da Chefia, bem como autorização da Diretoria Administrativa, para a produção intelectual científica de Trabalho de Conclusão de Curso – TCC intitulado "O ARQUIVISTA NA ERA DIGITAL: a implementação de medidas de segurança da informação em ambientes digitais e sua participação no processo de elaboração de políticas de segurança da informação", do graduando em arquivologia pela UEPB **Douglas Nascimento de Santana**, sob orientação da Profa. Ma. Gerlane Farias Alves.

Essa autorização se faz necessária, tendo em vista que o referido graduando utilizará de informações presentes no âmbito do Tribunal de Justiça da Paraíba para compor o relato de experiência, com o objetivo de analisar o papel do arquivista na usabilidade do RDC-arq. A pesquisa diz respeito à prática da preservação digital e os cuidados necessários para manter a autenticidade e a confiabilidade da informação no âmbito eletrônico, abordando a prática e a importância da preservação digital e os cuidados necessários adotados pelo Tribunal de Justiça da Paraíba. Dessa forma, será necessário o uso de imagens que serão utilizadas para compor a pesquisa que resultará em uma Monografia.

Atenciosamente,
Gerlane Farias Alves
Professora de Arquivologia UEPB

Auricélia Maria da Silva
Chefe do Arquivo do Fórum Cível-JP
Matrícula 179.154-2
19-06-24

Assinatura do Chefe(a) do Setor