Preservação e segurança da informação: desafios para assegurar a memória e o patrimônio

Preservación y seguridad de la información: desafíos para asegurar la memoria y el patrimonio

Priscila Lopes Menezes[1] https://orcid.org/0000-0002-5973-3351
Francisco Carlos Paletta[2] https://orcid.org/0000-0002-4112-5198
Terezinha Elisabeth da Silva[3] https://orcid.org/0000-0002-6176-7462

[1] Universidade Estadual de Londrina, Brasil, priscila.menezes@uel.br.
[2] Universidade Estadual de Londrina, Brasil, fcpaletta@usp.br.
[3] Universidade Estadual de Londrina, Brasil, terezinha.elisabeth.silva@gmail.com.

Resumo

O artigo objetiva refletir sobre a necessidade de atenção para perda da memória institucional e o patrimônio informacional e cultural, a partir de elementos que envolvem a segurança da informação. Fundamentado no construcionismo social, com abordagem qualitativa, apresenta pesquisa bibliográfica e documental referente à memória e patrimônio, preservação e segurança da informação pautada em pessoas, processos (diretrizes, normas, políticas, legislação) e ferramentas (recursos físicos e lógicos). Apresenta como questionamento, qual o papel da gestão da informação em evidenciar os elementos que compõem a preservação e segurança dos acervos? Considera que os ataques cibernéticos, alagamentos, incêndios e diferentes ameaças e vulnerabilidades têm gerado riscos na manutenção da memória e do patrimônio histórico, prejudicando a disponibilidade da informação para as gerações atuais e futuras. Conclui que a implantação de Sistemas de Gestão de Segurança da Informação é a recomendação indicada para proteger e garantir o acesso aos acervos. Destaca a necessidade de sensibilizar os gestores responsáveis por unidades de informação quanto à demanda associada à preservação da memória e do patrimônio histórico, de processos que sejam norteadores para a execução contínua da segurança informacional e ferramentas que possam ser utilizadas a longo prazo pelas instituições.

Palavras-chave: MEMÓRIA; PATRIMÔNIO; SEGURANÇA DA INFORMAÇÃO; PRESERVAÇÃO DA MEMÓRIA E PATRIMÔNIO.

Resumen

El artículo pretende reflexionar sobre la necesidad de prestar atención a la pérdida de la memoria institucional y del patrimonio informativo y cultural, a partir de elementos que tienen que ver con la seguridad de la información. Basado en el construccionismo social, con enfoque cualitativo, presenta investigaciones bibliográficas y documentales sobre memoria y patrimonio, preservación y seguridad de la información basadas en personas, procesos (directrices, normas, políticas, legislación) y herramientas (recursos físicos y lógicos). Como pregunta, ¿cuál es el papel de la gestión de la información a la hora de poner de relieve los elementos que componen la preservación y seguridad de las colecciones? Considera que los ciberataques, inundaciones, incendios y diferentes amenazas y vulnerabilidades han generado riesgos en el mantenimiento de la memoria y el patrimonio histórico, perjudicando la disponibilidad de la información para las generaciones actuales y futuras. Concluye que la implantación de Sistemas de Gestión de la Seguridad de la Información es la recomendación indicada para proteger y garantizar el acceso a las colecciones. Destaca la necesidad de concienciar a los gestores responsables de las unidades de información sobre la exigencia asociada a la preservación de la memoria y el patrimonio histórico, de los procesos que sirven de guía para la implantación contínua de la seguridad de la información y de las herramientas que pueden ser utilizadas a largo plazo por las instituciones.

Palabras clave: MEMORIA; PATRIMONIO; SEGURIDAD DE LA INFORMACIÓN; PRESERVACIÓN DE LA MEMORIA Y EL PATRIMONIO

Abstract

The article aims to reflect on the need for attention to the loss of institutional memory and the informational and cultural heritage, from elements involving information security. Based on the social constructionism, with qualitative approach, presents bibliographic and documentary research on memory and heritage, preservation and information security based on people, processes (guidelines, standards, policies, legislation) and tools (physical and logical

resources). It presents as a question, what is the role of information management in highlighting the elements that make up the preservation and security of collections? It considers that cyber attacks, floods, fires and different threats and vulnerabilities have generated risks in the maintenance of the memory and the historical heritage, harming the availability of the information for the current and future generations. It concludes that the implementation of Information Security Management Systems is the recommendation indicated to protect and guarantee the access to the collections. It highlights the need to raise awareness of managers responsible for information units regarding the demand associated with the preservation of memory and historical heritage, of processes that are guidelines for the continuous implementation of information security and tools that can be used in the long term by institutions.

Keywords: MEMORY; HERITAGE; INFORMATION SECURITY; PRESERVATION OF MEMORY AND HERITAGE.

1 Introdução

A humanidade tem como marca a destruição de seus registros documentais, seja por catástrofes naturais, guerras, bombardeios, e até por motivos religiosos, como ocorreu no período da inquisição, resultando na perda da memória, do patrimônio documental e cultural.

Somado a esses fatores, as unidades informacionais esbarram no desinteresse dos gestores em manter os acervos preservados, na falta de recursos financeiros, humanos, políticos e administrativos que deveriam ser direcionados para a salvaguarda de acervos. A predominância das ações dos dirigentes tem sido no uso dos registros fundamentados no hoje e não a longo prazo, principalmente ao que diz respeito aos dados digitais, que apresentam ambientes sensíveis, sem infraestruturas confiáveis.

O mês de abril de 2021 demonstra que essas situações não dizem respeito somente ao passado, mas permanecem acontecendo. Exemplos brasileiros disso é o ataque *hacker* iniciado no dia 11/04/21, no *site* da Fundação Biblioteca Nacional, que manteve a página da instituição fora do ar por mais de 15 dias, devido ao risco de

infecção à integridade do acervo, além de ter comprometido 5% dos dados digitais (GONÇALVES, 2021). Também, o manifesto dos trabalhadores da Cinemateca Brasileira, datado em 12/04/21, contendo um alerta sobre os riscos que a ausência de tratamento técnico no acervo o sujeitava, além da falta de manutenção do maquinário, das bases de dados e do prédio (JOAQUIM, 2021). Fatores que devido à ausência de providências, acarretaram o incêndio do órgão no dia 29/07/21, resultando na perda de aproximadamente quatro toneladas do acervo audiovisual do cinema brasileiro e no fechamento do prédio por aproximadamente dois anos, desde agosto de 2020 até maio de 2022 (G1 SP; TV GLOBO, 2021; VALERY, 2022). Outro episódio foi o incêndio que atingiu o prédio da reitoria da Universidade Federal do Rio de Janeiro (UFRJ), no dia 20/04/21, no qual estima-se a perda de sete mil periódicos da segunda metade do século XX sobre a história da arquitetura no Brasil, que fazem parte do acervo do Núcleo de Pesquisa e Documentação da Faculdade de Arquitetura e Urbanismo (NPD/ FAU) (YONESHIGUE; LYRA, 2021). E, ainda, no dia 28/04/2021, a invasão *hacker* no Tribunal de Justiça do Rio Grande do Sul (TJRS) que manteve as redes internas do órgão inacessíveis, além de ser necessário suspender o expediente externo e prazos processuais do TJRS (ROCHA, 2021).

Tais exemplos trazem como questionamento qual o papel da gestão da informação em evidenciar os elementos que compõem a preservação e segurança dos acervos? Independente dos variados formatos, todos os fatos demonstram que a perda dos dados são expressivas e geram lacunas para a construção da memória da sociedade.

Báez (2004), em seu livro “História Universal da Destruição dos Livros - das Tábuas Sumérias à Guerra do Iraque” apresenta o histórico de quanto o patrimônio documental já foi transformado em ruínas e utiliza o termo “genocídio cultural” para relatar o irreparável dano para as gerações futuras quanto a extinção documental.

Nesse sentido, o objetivo deste artigo é refletir sobre a necessidade de atenção para perda da memória institucional, a partir de elementos que envolvem a segurança da informação (SI), bem como, do patrimônio informacional e cultural. O trabalho se justifica devido ao entendimento que a Gestão da Informação inclui a proteção dos acervos e o seu uso seguro. Gerir os ativos informacionais envolvem o estabelecimento de controles, de processos e estruturas que necessitam ser

implementadas, monitoradas e melhoradas, incidindo na confiabilidade e durabilidade dos acervos.

2 Metodologia

O artigo tem o viés ligado ao construcionismo social, que percebe a sociedade e os processos interconectados, de modo que as situações estudadas não são distantes, mas influenciam o cotidiano dos pesquisadores. Presta-se atenção nas relações e mudanças que ocorrem nas organizações sociais que afetam e são afetados pelo todo, tirando o foco da estabilidade (BECKER, 2007).

Caracteriza-se como pesquisa bibliográfica e documental, com abordagem qualitativa, sem levantamento exaustivo do tema. Fez-se uso do portal da Capes, sem especificação de base de dados, nos meses de abril e maio de 2021, utilizando os termos de pesquisa “preservação documental” *and* “memória institucional” *and* “segurança da informação”, com datas-limite entre 2010 a 2021, refinado por periódicos revisados por pares, em que se obteve um resultado de 60 artigos científicos. A delimitação foi escolhida visando obter pesquisas com resultados recentes sobre o assunto. Além de legislação, reportagens jornalísticas, dissertação, tese e normas que atendessem a temática foram localizadas pelo Google.com. A partir dessa fase, seguiu-se para o fichamento, seleção e análise dos textos a partir da leitura na íntegra dos artigos que fariam parte do *corpus* da pesquisa, buscando aprofundar o entendimento sobre o tema.

3 Memória e patrimônio

É sabido que a função das unidades informacionais é preservar a memória institucional, enquanto fontes de prova, para que estas sejam propagadas e cheguem até o usuário. Quando se fala em memória, Souza e Morigi (2020, p. 229) a conceituam como:

> [...] a capacidade de rememorar fatos, acontecimentos. Todavia, quando a memória humana já não suporta mais guardar a grande quantidade de informações, excedendo sua capacidade, é necessário o uso da memória artificial, que são os suportes e os dispositivos informacionais que nos facilitam a ação de recordar.

Pode-se entender aqui que tal memória artificial fica armazenada nos arquivos, centros de documentação, bibliotecas e museus, locais onde a recuperação e resguardo das recordações de uma nação estariam mais facilmente disponíveis. Em outras palavras, as instituições mencionadas preservam registros de diversas naturezas e suportes, que são representativos para a reconstrução de vivências e saberes de toda humanidade e, a partir de sua preservação é possível compreender as ações, rotinas e cultura de todo um grupo de pessoas (SOUZA; MORIGI, 2020).

O conjunto de relações internas e externas que englobam as trajetórias sociais e históricas das unidades de informação, que fortalecem a cultura organizacional e auxilia na tomada de decisão é entendida como a memória institucional (PRADO; GRACIOSO; COSTA, 2019). Marcial e Vieira (2021) destacam que a preservação de documentos relacionados à memória institucional é tida como complexa e marcada por esquecimentos a fim de obscurecer dados, em que a gestão de documentos físicos e digitais são desafiadores, levando em consideração que o tempo de vida dos suportes informacionais podem ser de somente meses.

Conforme apontado por Báez (2004), quando o desejo era “zerar o passado”, eram provocadas grandes queimas de acervos arquivísticos e bibliográficos. Por este motivo fala-se na preservação do patrimônio informacional e cultural, pois eles trazem à tona a compreensão do presente por meio do passado.

Vale lembrar que o patrimônio documental envolve a documentação de guarda permanente, que apresenta valor histórico-cultural, sendo capaz de constituir a identidade de um povo, a partir das fontes preservadas (ROSA; BAPTAGLIN, 2018). O patrimônio documental é constituído e entendido como conjunto de bens com valores diversificados que justificam a sua preservação por apresentar a história das populações, ascendendo a memória coletiva e individual para a construção de aspectos artísticos, científicos e culturais (LAGE, 2002).

E sobre patrimônio cultural, Báez (2004) menciona que se deve entendê-lo como algo que causa o sentimento de pertencimento de um povo, aquilo que faz recordar uma identidade, propiciando ações de integração, visto como um bem coletivo. O patrimônio documental está inserido em um contexto cultural e de conservação que se relaciona com a memória. Sendo assim, Dodebei (2015) apresenta que memória e patrimônios são processos interligados, que não podem ser vistos de maneira

isolada, pois a memória pode vir a ser patrimônio e o patrimônio precisa da memória para se justificar no tempo.

Conforme as “Diretrizes para a Salvaguarda do Patrimônio Documental do Programa Memória do Mundo da Unesco” (2002), existem itens e coleções documentais que precisam estar acessíveis a qualquer tempo, para o mundo todo, tendo em vista que são heranças das gerações atuais e futuras. A fim de que a memória não se perca e exista acessibilidade permanente aos registros, são necessários esforços coletivos direcionados à preservação dos acervos e é diante disso que se fala na segurança da informação.

4 Elementos de preservação e segurança da informação

As instituições, cientes do valor informacional que produzem e fazem uso, também dos riscos e vulnerabilidades com que estão expostas, a fim de garantir a continuidade de seus negócios preocupam-se em proteger a informação, ou seja, a partir de Sistemas de Gestão de Segurança da Informação (SGSI) procuram assegurar as propriedades de confidencialidade, integridade e disponibilidade de seus dados (ABNT, 2013).

Conforme o art. 2º do Decreto n. 9.637, de 26/12/2018, que Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação a SI abrange:

> I - a segurança cibernética;
> II - a defesa cibernética;
> III - a segurança física e a proteção de dados organizacionais; e
> IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação (BRASIL, 2018, p. 1).

Desse modo, o decreto, não se dirige exclusivamente aos acervos digitais, mas engloba todos os riscos que os registros informacionais sofrem e se expõem. Sendo possível ainda destacar dentre os objetivos do Plano Nacional de Segurança da Informação, que constam no art. 4º, o inciso VII: “contribuir para a preservação da memória cultural brasileira” (BRASIL, 2018, p. 2).

Nesse sentido, teoricamente, está expressa a necessidade de possibilitar o acesso às informações, função nata das unidades informacionais, a partir de registros íntegros e autênticos, em que se possa confiar em seu valor de prova, e no caso de dados

com valores primários, aborda a confidencialidade, em que se assegura a proteção dos dados.

Zapater e Suzuki (2005), e Almeida, Souza e Cardoso (2010) também reforçam que a gestão da segurança da informação não se limita às ferramentas tecnológicas ou dados em formatos digitais, mas compreende uma visão geral das instituições onde os fornecedores e usuários da informação fazem parte, os processos e as ferramentas precisam igualmente ser analisados, bem como, a natureza física, política e cultural do ambiente organizacional.

Portanto, neste artigo, far-se-á uso de três eixos para o tratamento da segurança da informação: as pessoas, os processos e as ferramentas. Vistos como complementares e interdependentes, responsáveis por garantir a produtividade e a qualidade nas instituições (ZAPATER; SUZUKI, 2005).

4.1 As pessoas

Em todas as organizações, pessoas internas e externas ao órgão têm envolvimento com a informação e, portanto, são responsáveis pela segurança dos dados. Conforme apontado pela Unesco (2002), toda sociedade interessada em proteger os acervos e perpetuar a história tem responsabilidade em salvaguardar o patrimônio, sugerindo até mesmo que disciplinas que fomentem a preservação patrimonial sejam incluídas nos currículos escolares.

Tal sugestão está ligada à ideia de sensibilização das pessoas, o que não difere das campanhas, das capacitações e dos folhetos educativos que devem ser utilizados para conscientização de servidores nas instituições. Os funcionários são os principais envolvidos nas atividades cotidianas dos órgãos, sendo capazes de determinar o que deve ser protegido, com qual prioridade, com quais recursos e destacam condutas básicas que são diferenciais no planejamento da segurança (ALMEIDA; SOUZA; CARDOSO, 2010). Zapater e Suzuki (2005) mencionam que a solução não é monitorar integralmente as atividades das pessoas, mas a partir de treinamentos e campanhas alertar para vulnerabilidades.

Santos (2012) argumenta que um dos recursos para evitar a perda das informações, sem aumentar os custos financeiros, é fazer uso do compartilhamento do conhecimento individual de cada pessoa que trabalha nos órgãos. Muitas vezes o

servidor possui as habilidades para sugerir ideias, mas não é ouvido. A autora acredita que com a ênfase no compartilhamento de informações dentro das unidades, as decisões tomadas nas instituições serão feitas de maneira reflexiva, resultando na otimização dos processos e uso adequado das informações.

A alta administração também precisa estar envolvida no desenvolvimento, implementação e monitoramento do SGSI, pois são os responsáveis por destinar os recursos necessários as ações, realocar serviços e otimizar estratégias (MISHRA, 2015).

Outro fator destacado por Galegale, Fontes e Galegale (2017), diz respeito à importância de os órgãos possuírem um setor destinado ao SGSI, retratando a consciência quanto aos riscos à segurança informacional e assumindo o comprometimento de que a instituição conseguirá atingir seus objetivos sem percalços.

Enfim, quem produz e utiliza as informações são peças-chave para atingir um SGSI com êxito, as pessoas são os sustentadores de um órgão, sendo necessário o reconhecimento das atividades de cada um para que haja um esforço voluntário em proteger o patrimônio.

4.2 Os processos

Os processos possuem papel principal no SGSI, pois englobam as políticas, os procedimentos, as diretrizes e as normas de conformidade. Portanto, é onde se encontra a direção e o padrão mínimo do como fazer (ZAPATER; SUZUKI, 2005).

A ISO/IEC 27002:2013 tem sido a norma técnica mais utilizada e referenciada como modelo estrutural para o SGSI (GALEGALE; FONTES; GALEGALE, 2017), podendo ser utilizada por instituições de todos os tipos e tamanhos, ela oferece uma diversificada série de controles, prometendo um projeto seguro para sistemas de segurança da informação (ABNT, 2013).

A norma contempla 19 seções (0 a 18), da primeira até a quarta com informações introdutórias e as 14 seguintes, que englobam 35 objetivos de controles que se expandem em 114 controles recomendados (ABNT, 2013):

- Políticas de segurança da informação: 1 objetivo, 2 controles;

- ❖ Organização da segurança da informação: 2 objetivos, 7 controles;
- ❖ Segurança em recursos humanos: 3 objetivos, 6 controles;
- ❖ Gestão de ativos: 3 objetivos, 10 controles;
- ❖ Controle de acesso: 4 objetivos, 14 controles;
- ❖ Criptografia: 1 objetivo, 2 controles;
- ❖ Segurança física e do ambiente: 2 objetivos, 15 controles;
- ❖ Segurança nas operações: 7 objetivos, 14 controles;
- ❖ Segurança nas comunicações: 2 objetivos, 7 controles;
- ❖ Aquisição, desenvolvimento e manutenção de sistemas: 3 objetivos, 13 controles;
- ❖ Relacionamento na cadeia de suprimento: 2 objetivos, 5 controles;
- ❖ Gestão de incidentes de segurança da informação: 1 objetivo, 7 controles;
- ❖ Aspectos de segurança da informação na gestão da continuidade do negócio: 2 objetivos, 4 controles;
- ❖ Conformidade: 2 objetivos, 8 controles.

Vale frisar que apesar de todos os controles serem importantes, eles não seguem um padrão hierárquico, pois cada instituição tem as suas especificidades, sendo necessária a análise e avaliação de riscos que, juntamente com os servidores do órgão, são capazes de planejar e definir quais objetivos devem ser implantados (ABNT, 2013).

A ISO/IEC 27002:2013 é tomada como padrão para elaboração do gerenciamento de segurança da informação por ser uma norma adotada mundialmente. As instituições que objetivam obter a certificação em segurança da informação necessitam estar adequadas as práticas desta norma e serem auditadas conforme os padrões da ISO/IEC 27001:2013, que define os requisitos para um SGSI (GALEGALE; FONTES; GALEGALE, 2017).

Conforme apresentado por Fontes (2011), o planejamento consiste na primeira etapa para a implantação do SGSI, que se divide em dois aspectos: da política e da gestão de riscos. Quanto às políticas de segurança da informação, estas vão estar concentradas na ABNT NBR ISO/IEC 27002:2013 — Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. E sobre a gestão de riscos, a fundamentação está na ABNT NBR

ISO/IEC 27005:2019 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

As políticas são a base para a elaboração de outros documentos. Apontadas como referenciais para estabelecer os controles na SI, definem o escopo e os limites da gestão de riscos, sendo assim, precisam ser simples, claras, abrangentes e de fácil compreensão por todos os colaboradores do órgão, recebendo ampla divulgação (FONTES, 2011).

Mishra (2015) acrescenta a necessidade de uma política de comunicação com o objetivo de assegurar o cumprimento dos controles, em que sejam divulgadas as consequências do não cumprimento dos objetivos, pois os erros ao comunicar prejudicam a eficiência dos processos e causam conflitos na atuação dos servidores.

Quanto à gestão de riscos como parte integrante do SGSI, convém que ela seja implantada e opere de forma constante nas instituições. Isto é fundamental a fim de que os riscos sejam identificados, analisados, monitorados e reduzidos a níveis aceitáveis, principalmente aqueles identificados como de alto impacto ou alta probabilidade de ocorrência (ABNT, 2019).

Mascarenhas Neto e Araújo (2019) relatam que as vulnerabilidades e as ameaças podem ser causadas por diferentes fatores, decorrentes de causas naturais (provocadas por água, fogo, eletricidade, entre outras) e causas humanas (divididas em acidentais e intencionais). Sendo assim, as organizações devem se ater em analisar e avaliar os riscos, preparando-se para diversificados cenários, em que, caso algum dano venha acontecer, o tempo de resposta, com o plano de gestão de riscos, será o menor possível. Conforme a ABNT (2019), o gerenciamento de riscos no SGSI tem o objetivo de impedir o comprometimento dos ativos da organização, estimando e propondo as mudanças necessárias nos requisitos de segurança, sendo capaz de gerar resultados otimizados.

4.3 As ferramentas

As ferramentas dizem respeito aos recursos físicos e lógicos empregados no SGSI, pois além de pessoas treinadas e processos bem elaborados, é útil o investimento em recursos tecnológicos como facilitador para as soluções que envolvem a

segurança, em que o foco não seja somente a detecção de ameaças, mas sua prevenção (ZAPATER; SUZUKI, 2005).

Assim como a tecnologia amplia as vulnerabilidades e perdas (adulterações, roubos, inautenticidades) que os registros das instituições podem sofrer, seu uso deve ser otimizado para promover uma rede maior de segurança aos dados. Ainda é recorrente o pensamento de gestores de que a digitalização ou os documentos nato digitais resolvem todos os problemas enfrentados pelos suportes convencionais. No entanto, cabe frisar o entendimento de Innarelli (2020, p. 42) de que:

> O suporte de armazenamento de todo e qualquer documento digital é produzido em meio físico, ou seja, ele é uma mídia de armazenamento, seja uma mídia magnética, seja uma mídia ótica, seja qualquer outro tipo de mídia. E essas mídias, esses suportes digitais, eles também são afetados por todos os elementos que tradicionalmente afetam a documentação convencional com a qual trabalhamos hoje em dia.

Innarelli (2020) e Flores (2020) têm o consenso de que a preservação dos documentos digitais precisa ser realizada desde a primeira fase do ciclo de vida documental, sendo necessárias cadeias de custódia ininterruptas que atendam aos requisitos arquivísticos, com a finalidade de manter os dados autênticos e confiáveis por longos períodos. Ao se trabalhar com *softwares*, *hardwares* e suportes da informação é preciso lembrar que o ciclo de obsolescência é rápido, no geral, de quatro a seis anos. Portanto, a infraestrutura não pode ser frágil, mas apresentar bons equipamentos e suportes de armazenamento (INNARELLI, 2020).

As instituições, de maneira geral, produzem os documentos em meio digital e não se preocupam com a segurança jurídica desses dados, em como será feita a transmissão e recolhimento desses ao longo do tempo, nem mesmo como esses documentos estão arquivados. Flores (2020) afirma que muitas vezes existe apenas uma *tag* de “arquivado”, sem atenção aos requisitos necessários à preservação e segurança digital.

Nesse sentido, o investimento em tecnologia é indispensável. Os programas e recursos digitais implantados precisam estar disponíveis e protegidos para que se configurem como utilitários aos órgãos. É perceptível que as ferramentas, os processos e as pessoas dependem um do outro para se ter êxito na implantação do SGSI, e o resultado é a proteção do patrimônio informacional e da memória.

5 Considerações finais

Diante do exposto, entende-se que para atingir a preservação e a segurança dos acervos em seus variados formatos é necessário o estabelecimento do SGSI nas unidades informacionais fundamentado no tripé: pessoas, processos e ferramentas.

O papel da gestão da informação em evidenciar os elementos que compõem a preservação e segurança dos acervos está diretamente relacionada com a perpetuação do patrimônio e da memória. É fundamental convencer e sensibilizar os administradores sobre a necessidade de rotinas de segurança da informação para que estas não se percam, nem sejam adulteradas. Destaca-se que existem registros que necessitam de prazo de guarda permanente, e que simplesmente digitalizar, sem critérios, não é a solução para garantir sua preservação e acesso.

O esperado dos profissionais da informação é o desenvolvimento de atividades que conservem, preservem, defendam e promovam o conhecimento do patrimônio informacional, como forma de manter a memória viva, difundindo como ela é construída. Os processos, ao contemplar as políticas, os procedimentos, as diretrizes, as legislações e as normas são os norteadores para o SGSI, traçando estratégias a longo prazo que visem garantir a preservação dos acervos que se cruzam com a história de cada pessoa, cidade, estado e país. Quanto às ferramentas, vale reforçar a necessidade de atenção quanto as escolhidas para fazer parte do SGSI, primando por aquelas que garantam a segurança dos dados, sem seleções imediatistas, que coloquem em risco a integridade dos registros informacionais.

Por fim, as situações apresentadas neste artigo cumprem o objetivo proposto de refletir sobre a necessidade de atenção para perda da memória institucional e do patrimônio informacional e cultural, a partir de políticas e estratégias de preservação e conservação, bem como, na definição de abordagem fundamentada no SGSI. Fica como sugestão para pesquisas futuras que se investigue a aplicação de melhores práticas associadas à guarda do patrimônio informacional.

Referências

Almeida, M. B.; Souza, R. R.; Cardoso, K. (2010). Uma proposta de ontologia de domínio para segurança da informação em organizações. *Informação e Sociedade: Estudos, 1* (20), pp-pp. 155-168. Recuperado de: https://brapci.inf.br/_repositorio/2010/09/pdf_91d3c5b818_0011848.pdf.

Associação Brasileira de Normas Técnicas. (2013). *Tecnologia da informação: Técnicas de segurança: Código de prática para a gestão da segurança da informação*. (NBR ISO/IEC 27002:2013) ABNT.

Associação Brasileira de Normas Técnicas. (2019). *Tecnologia da informação: Técnicas de segurança: Gestão de riscos de segurança da informação.* (NBR ISO/IEC 27005:2019) ABNT.

Báez, F. (2004). *História universal da destruição dos livros: das tábuas sumérias à Guerra do Iraque.* Rio de Janeiro: Ediouro.

Becker, H. S. (2007). *Segredos e truques da pesquisa.* Rio de Janeiro: Zahar.

Brasil. Presidência da República. Casa Civil. (2018) *Decreto n. 9.637, de 26 de dezembro de 2018.* Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto n. 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei n. 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Casa Civil. Recuperado de: https://cutt.ly/10kKGo5**.**

Dodebei, V. (2015). Tempos memoriais e patrimoniais: notas de pesquisa sobre memória e informação. In Azevedo Netto, C. X. de (Org.). *Informação, patrimônio e memória: diálogos interdisciplinares*. (pp. 44 – 64). João Pessoa: Editora da UFPB. Recuperado de: https://cutt.ly/Q0kKXec.

Flores, D. (2020, julio 29). Preservación de Archivos para el aseguramiento de la Información y la transparencia. [Apresentação de trabalho] *II Seminario de Archivos, Derechos Humanos, Memoria Histórica y Transparencia*, Bogotá, Colômbia. Recuperado de: https://cutt.ly/T0kKB9k.

Fontes, E. L. G. (2011). *Política de segurança da informação: uma contribuição para o estabelecimento de um padrão mínimo*. (Mestrado em Tecnologia) - Centro Estadual de Educação Tecnológica Paula Souza, São Paulo. Recuperado de: encurtador.com.br/cdpL2.

G1 SP; TV GLOBO. (2021, julho 29). Bombeiros controlam incêndio em galpão da Cinemateca Brasileira na Vila Leopoldina, Zona Oeste de SP; veja vídeos. *G1*. Recuperado em: encurtador.com.br/glEJQ.

Galegale, N. V.; Fontes, E. L. G.; Galegale, B. P. (2017, julho/setembro). Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. *Perspectivas em Ciência da Informação, 22* (3), pp-pp. 75-97. Recuperado de: https://shre.ink/1Ub1.

Gonçalves, A. L. D. (2021, abril 28). Site da Biblioteca Nacional volta ao ar após ataque hacker. *Tecmundo*. Recuperado de: https://shre.ink/1UbF.

Innarelli, H. (2020). Sinistros em ambientes digitais de arquivos. *Revista do Arquivo, 7* (11), pp-pp. 41-49. Recuperado de: encurtador.com.br/dgrs1.

Joaquim, L. (2021, abril 13). Manifesto dos trabalhadores da Cinemateca. *Cinema escrito*. Recuperado de: encurtador.com.br/klzU3.

Lage, M. O. P. (2002). Abordar o património documental: territórios, práticas e desafios. Guimarães: NEPS. (Cadernos NEPS; n.º 4). Recuperado de: https://shre.ink/1Ubm.

Marcial, E.; Vieira, J. da S. (2021). Memória institucional em Risco. *Revista Ibero-Americana de Ciência da Informação, 14* (1), pp-pp. 150–170. Recuperado de: https://shre.ink/1UbX.

Mascarenhas Neto, P. T.; Araújo, W. J. (2019). *Segurança da informação: uma visão sistêmica para implantação em organizações.* João Pessoa: Editora UFPB.

Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. *Information & Computer Security, 23* (2), pp-pp. 122-144. Recuperado de: encurtador.com.br/gotAJ.

Prado, S.; Gracioso, L. S.; Costa, L. S. F. (2019). O papel da memória institucional para a gestão universitária: contribuições para a consolidação da UMMA na UFSCar. *Informação & Informação, 24* (3), pp-pp. 409-432. Recuperado de: encurtador.com.br/GMSY2.

Rocha, J. (2021, maio 4). TJ-RS segue trabalhando para restabelecer sistemas operacionais após ataque hacker. *Jornal do Comércio*. Recuperado de: https://shre.ink/1gUL.

Rosa, T. C.; Baptaglin, L. A. (2018). Acesso à informação e ao patrimônio documental da Universidade Federal de Roraima: uma reflexão

necessária. *Archeion Online*, *6* (1), pp-pp. 3-22. Recuperado de: https://shre.ink/1gU1.

Santos. A. P. (2012, janeiro/junho). Amnésia Organizacional: um Estudo de Caso Sobre a Memória na Administração Pública Federal. *InCID: R. Ci. Inf. e Doc.*, *3* (1), pp-pp. 36-56. Recuperado de: https://shre.ink/1gUe.

Souza C. A. De; Morigi V. J. (2020, setembro 13). Memória e instituição: os registros da Associação de Ex-alunos do Instituto de Educação General Flores da Cunha (Porto Alegre- RS, Brasil). *Logeion: Filosofia da Informação*, *7* (1), pp-pp. 228-243. Recuperado de: https://shre.ink/1gUD.

UNESCO. (2002). *Programa Memória do Mundo: Diretrizes para a salvaguarda do patrimônio documental.* Elaborado para Unesco por Ray Edmondson. Divisão da Sociedade da Informação/Unesco. Recuperado de: https://shre.ink/1gUp.

Valery, G. (2022, maio 09). Cinemateca Brasileira marca data para reabrir após dois anos de desmonte. *Brasil de Fato*. Recuperado de: https://abre.ai/fwkA.

Yoneshigue, B.; Lyra, J. C. (2021, abril 23). Incêndio na UFRJ: conheça o acervo histórico de arquitetura que quase foi perdido. *Extra*. Recuperado de: https://shre.ink/1gr0.

Zapater, M.; Suzuki, R. (2005). Segurança da Informação: um diferencial determinante na competitividade das corporações. *Promon Business & Technology Review*. Recuperado de: https://shre.ink/1gr4.