Biblios
E-ISSN: 1562-4730
editor@bibliosperu.com
Julio Santillán Aldana, ed.
Perú

Fernandes Belarmino, Valdete; Junqueira de Araújo, Wagner
Análise de vulnerabilidades computacionais em repositórios digitais
Biblios, núm. 56, 2014, pp. 1-18
Julio Santillán Aldana, ed.
Lima, Perú

Biblios
ISSN 1562-4730 (online)

Análise de vulnerabilidades computacionais em repositórios digitais

Valdete Fernandes Belarmino
Wagner junqueira de Araújo

Universidade Federal da Paraíba – UFPB, Brasil

ANALYSIS

Resumo

Objetivo. Apresenta os resultados de pesquisa que teve como objetivo analisar as vulnerabilidades computacionais dos diretórios digitais das universidades públicas. Destaca a relevância da informação na sociedade contemporânea como um recurso de valor inestimável, enfatizando a informação científica como elemento essencial para constituir o progresso científico. Caracteriza o surgimento dos Repositórios Digitais e ressalta sua utilização em meio acadêmico para preservar, divulgar, disseminar e incentivar a produção científica. Descreve os principais softwares para a construção de repositórios digitais.
Método. A pesquisa identificou e analisou as vulnerabilidades que estão expostos os repositórios digitais institucionais em das universidades em âmbito federal, por meio da execução de Testes de Penetração, especificando os níveis de riscos e os tipos de vulnerabilidades.
Resultados. De uma amostra de 30 repositórios, foi possível analisar 20, sendo identificados que: 5% dos repositórios possuem vulnerabilidades críticas, 85% altas, 25% médias e 100% baixas.
Conclusões. Evidencia a necessidade da adoção de medidas para estes ambientes que promovam a segurança dos ativos informacionais, visando minimizar a incidência de ataques externos e/ou internos aos sistemas das instituições.

Palavras-chave
Segurança da Informação ; Repositórios digitais ; DSpace ; Informação científica ; Preservação digital ; Teste de penetração

Analysis of computational vulnerabilities in digital repositories

Abstract

Objective. Demonstrates the results of research that aimed to analyze the computational vulnerabilities of digital directories in public Universities. Argues the relevance of information in contemporary societies like an invaluable resource, emphasizing scientific information as an essential element to constitute scientific progress. Characterizes the emergence of Digital Repositories and highlights its use in academic environment to preserve, promote, disseminate and encourage the scientific production. Describes the main software for the construction of digital repositories.
Method. The investigation identified and analyzed the vulnerabilities that are exposed the digital repositories using Penetration Testing running. Discriminating the levels of risk and the types of vulnerabilities.
Results. From a sample of 30 repositories, we could examine 20, identified that: 5% of the repositories have critical vulnerabilities, 85% high, 25% medium and 100% lowers.
Conclusions. Which demonstrates the necessity to adapt actions for these environments that promote informational security to minimizing the incidence of external and / or internal systems attacks.Abstract Grey Text – use bold for subheadings when needed.

Keywords
Information Security ; Digital repositories ; DSpace ; Scientific information ; Digital preservation ; Penetration test

Introdução

A informação é um bem de valor inestimável para a sociedade e um recurso absolutamente necessário para adquirir conhecimento. O elemento fundamental para estabelecer o progresso científico, tecnológico e educacional de uma nação é a informação científica. Esse tipo de informação é revelado à sociedade através dos periódicos científicos, em consequência do trabalho intelectual dos pesquisadores (KURAMOTO, 2006).

No decorrer dos tempos, o avanço tecnológico e o processo de globalização possibilitaram a integração e o compartilhamento de informações de maneira instantânea, resultando em um aumento de publicações considerado acima do comum. A publicação de artigos em revistas científicas sustenta um ciclo produtivo que se transforma em um recurso indispensável para o sistema de comunicação científica.

Com o crescimento exponencial bibliográfico (em suporte tradicional, o papel, e em maior escala, no formato digital) e a facilidade na produção de novas informações em ambiente virtual, a quantidade de material eletrônico disponível para acesso na internet é amplamente variada. Só de artigos científicos em CI, o crescimento da produção acadêmica a partir do ano 2001 até o segundo semestre de 2013 representa aproximadamente 63%, de acordo com dados disponíveis na Base de Dados Referencial de Artigos de Periódicos em Ciência da Informação – BRAPCI[1].

Tal crescimento, foi auxiliado com o surgimento dos Repositórios Digitais (RDs), que além de artigos abrigam os resultados de trabalhos de conclusão de curso, dissertações, teses, anais de encontros científicos, palestras etc. As instituições acadêmicas utilizam os repositórios digitais para divulgar, disseminar, preservar e incentivar a produção científica de sua comunidade. As tecnologias aliadas à disseminação da informação assumem um papel crucial na sociedade do conhecimento. Por ser um componente valioso no desenvolvimento do saber do indivíduo, existe uma preocupação coletiva com o tratamento, a preservação, a disseminação e a segurança da informação.

A construção e manutenção de repositórios digitais exigem das instituições recursos computacionais, pessoas habilitadas e processos para a gestão. Existe um estudo que aborda a segurança em itens relativos a pessoas e processos (LIMA; LIMA, 2012), contudo não aborda os aspectos de segurança do ambiente computacional.

Diante do exposto, surgiu a seguinte questão de pesquisa: como estão configurados os elementos de segurança da informação no ambiente computacional dos repositórios digitais das universidades federais no Brasil?

Este artigo apresenta o resultado de pesquisa tem como objetivo geral analisar a segurança da informação no ambiente computacional dos repositórios institucionais digitais no âmbito das universidades federais. De forma a discutir os aspectos característicos da segurança da informação; identificar os tipos de vulnerabilidades que os repositórios digitais estão expostos e indicar estratégias para evitar e/ou reduzir os riscos/ameaças à segurança da informação. Para fins deste estudo entende-se como ambiente computacional os elementos de configuração de software usados para implementar os sistemas de repositórios digitais.

1 Repositórios digitais

O Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT)[2] define em sua página na internet que os repositórios digitais (RDs) são bases de dados *online* que reúnem de maneira organizada a produção científica de uma instituição ou área temática. De maneira complementar, Weitzel (2006b) especifica a divisão dos repositórios digitais em categorias: institucionais ou temáticos. Os primeiros dizem respeito à organização e acesso à produção científica de uma instituição, enquanto os segundos são atribuídos a uma determinada área do conhecimento.

Considerando que os repositórios possibilitam a gestão da produção intelectual científica e acadêmica em qualquer tipo de arquivo digital, Viana, Márdero Arellano e Shintaku (2005, p. 3), completam que: “um repositório digital é uma forma de armazenamento de objetos digitais que tem a capacidade de manter e gerenciar material por longos períodos de tempo e prover o acesso apropriado.” Para fortalecer o conceito, Ribeiro e Vidotti (2009, p. 106), destacam:

> Os repositórios digitais trazem a ideia de preservação dos objetos digitais, além de promover o acesso livre a conteúdos como produtos de pesquisa, entre outros. Além disso, esses repositórios precisam ser criados tendo como necessidades dos usuários potenciais, permitindo usabilidade e acessibilidade satisfatórias.

Portanto, os repositórios digitais são bases de dados quem contêm toda variedade de objetos em formato digital (documento de texto, imagem, áudio, vídeo etc.), com a finalidade de disseminar o conteúdo informacional de forma mais estruturada e tornar sua recuperação acessível em longo prazo por qualquer pesquisador.

> Os repositórios digitais oferecem muitos benefícios em relação aos serviços digitais, auxiliando a comunidade científica na organização e aquisição de trabalhos científicos de uma determinada instituição ou comunidade, oferecendo acesso irrestrito, intercâmbios e troca de informações, bem como outros tipos de serviços e recursos. (CAMARGO, 2008, p. 14 apud RIBEIRO; VIDOTTI, 2009, p. 111-112).

Um repositório digital pode ser mantido por qualquer instituição, seja científica, acadêmica, governamental ou outro tipo de organização solidamente constituída, a qual tenha o propósito de promover a distribuição absoluta da informação, o livre acesso ao documento integral, o recurso de interoperabilidade e o atributo de armazenamento em longo prazo.

A página na internet do *Registry of Open Access Repositories* – ROAR[3] (Registro de repositórios de acesso aberto, em tradução livre) apresenta indicadores sobre os repositórios inscritos pelos provedores de serviços no mundo, onde é possível ordenar a lista de repositórios e especificar a busca por país, software utilizado e tipo de repositório determinado.

De acordo com esse registro em maio de 2013, o Brasil ocupa a 6ª posição na lista de países com mais repositórios digitais de acesso aberto no mundo (133), ficando atrás da Espanha (155), Japão (167), Alemanha (192), Reino Unido (249) e Estados Unidos (550).

2 Softwares para a construção de repositórios digitais

As plataformas usadas para a criação de repositórios digitais podem ser livres, com código aberto, comumente elaboradas por institutos, e/ou universidades e disponíveis de forma gratuita. Deste modo, estas ferramentas podem ser instaladas, avaliadas, utilizadas e customizadas irrestritamente por qualquer organização que tencione aplicá-las na constituição de uma biblioteca digital. (OLIVEIRA; CARVALHO, 2011).

A plataforma DSpace é uma das mais utilizadas para a construção de repositórios digitais. O DSpace foi concebido pelo *Massachusetts Institute of Technology* (MIT) em colaboração com a *Hewlett-Packard Company* (HP) entre março de 2000 e novembro de 2002 e ainda

> [...] foi traduzido em parceria com a equipe da PORTCOM (Rede de Informação em Comunicação dos Países de Língua Portuguesa) da INTERCOM (Sociedade Brasileira de Estudos Interdisciplinares da Comunicação) e do Núcleo de Pesquisa *Design de Sistemas Virtuais Centrado no Usuário* da USP (Universidade de São Paulo). (WEITZEL, 2006b, p. 5).

A ferramenta DSpace permite a criação de repositórios digitais para a captura da produção intelectual de organizações e instituições de pesquisa com funcionalidades de armazenamento, distribuição, visibilidade e preservação da informação, possibilitando sua customização por outras instituições que adotem esse sistema. O DSpace é uma ferramenta integrada para apoiar o planejamento de preservação digital em longo prazo e administrar o conteúdo depositado, o que o torna um software adaptado às realidades da gestão de um repositório em um grande cenário institucional.

Dentre suas características principais destacam-se: possuir uma arquitetura simples e eficiente, utilizar uma tecnologia de ponta, ser um software livre direcionado para o acesso aberto e ser propositadamente desenvolvido para servir de repositório institucional (VIANA; MÁRDERO ARELLANO; SHINTAKU, 2005). Além desses atributos, o DSpace apresenta a prerrogativa de utilizar "[...] identificadores persistentes que facilitam referenciar os objetos digitais por um longo período de tempo. O uso do Dspace tem se mostrado fácil e flexível, garantindo a preferência por esse *software* para a criação dos repositórios digitais." (RIBEIRO; VIDOTTI, 2009, p. 108-109).

O software EPrints também é bastante empregado na construção de repositórios digitais de acesso aberto no mundo. Desenvolvido pela Universidade de Southampton na Inglaterra, a primeira versão do sistema foi lançada publicamente no final no ano 2000. É um programa apropriado para a criação de repositórios institucionais ou

temáticos, oferecendo ampla rede de suporte para novas implementações. É um software livre, de código aberto, que dispões de mínimo conhecimento técnico para sua instalação e que pode ser facilmente modificado para satisfazer as preferências da instituição que o utilize.

Sobre os arquivos em formato digital que a ferramenta suporta, Viana e Márdero Arellano (2006, p. 4) destacam que "os repositórios baseados no EPrints permitem o depósito de pré-prints (trabalhos ainda não publicados), pós-prints (já publicados), outros tipos de publicações, comentários e versões, bem como de outros tipos de documentos." O IBICT customizou versões em português para os softwares DSpace e EPrints.

Outra opção é a ferramenta Fedora que foi idealizada em conjunto pelas Universidades de Virginia e Cornell, sendo igualmente um software livre de código aberto. O sistema oferece uma arquitetura projetada e acrescenta utilitários que facilitam o gerenciamento dos repositórios. Sobre a interface do sistema, Oliveira e Carvalho (2011, p. 8) ressaltam que:

> O núcleo central do Fedora é o repositório de serviços, que pode ser acessado utilizando interfaces via web service, que permite a criação, gerenciamento, armazenamento, acesso e o reuso dos objetos digitais. Todas as funções do Fedora, tanto no nível de administração do repositório como no nível do acesso aos objetos digitais são disponibilizados por este repositório de serviços.

De acordo com o ROAR, o Fedora é uma ferramenta utilizada pelos provedores de serviços, configurando na 5ª colocação no ranking de softwares aplicados na implementação de repositórios digitais. O sistema Fedora apresenta uma diferença em relação ao EPrints e ao DSpace por não possuir em sua plataforma básica uma interface completa com o usuário final. (OLIVEIRA; CARVALHO, 2011).

Dos softwares utilizados com mais frequência para a criação dos repositórios digitais em nível mundial conforme o ROAR destacam-se o DSpace (1350), EPrints (497), Bepress (175), OPUS (50) e Fedora (41).

3 Utilização do software DSPACE

A informação científica isenta de qualquer restrição de acesso e livre de ônus ao usuário, proporciona benfeitorias tanto para a instituição que a disponibiliza (com o aumento da sua visibilidade) quanto para o pesquisador, com a valorização do seu trabalho. Para Kuramoto (2008) esse modelo tecnológico que oferece o acesso aberto à produção intelectual mundial apresenta resultados importantes para o desenvolvimento científico dos países, como a facilidade de tornar internacional a literatura científica produzida localmente e a redução da exclusão cognitiva, bem como um maior compartilhamento do conhecimento produzido.

> A iniciativa de Arquivos Abertos e o Movimento de Acesso Aberto à Informação Científica vêm propondo que a informação científica seja disponibilizada gratuitamente; o que é favorecido pelos avanços constantes das tecnologias da informação e comunicação (TIC) dos últimos anos, gerando uma demanda do uso da *web* para a disseminação dos resultados de pesquisa. (FACHIN et al, 2009, p. 221).

Devido à OAI, o emprego dos repositórios digitais nos mais diversos tipos de instituições existentes (científicas, acadêmicas, governamentais, centros de pesquisa, organizações sem fins lucrativos, arquivos públicos, centros médicos etc.) vem crescendo exponencialmente em virtude dos seus inúmeros benefícios.

O software DSpace é uma das ferramentas mais utilizada mundialmente para a criação dos repositórios digitais de acesso livre. Os dados disponíveis no site do ROAR comprovam essa afirmação, constatando que há 1350 (até maio de 2013) repositórios digitais cadastrados em sua base que utilizam essa plataforma em todo o mundo. Por sua natureza operacional, o DSpace "é um dos softwares que apresenta condições mais propícias de preservação e acesso aos documentos armazenados." (TARGINO; GARCIA; PAIVA, 2012, p. 21).

Durante a pesquisa verificou-se que o Brasil possuía 133 repositórios digitais registrados nessa base de dados, dos quais 72 foram construídos com o uso do software DSpace, o que corresponde a aproximadamente 54% dos

repositórios do país. Com isso, o Brasil ocupa a 5ª posição entre os países que mais utilizam essa ferramenta para a construção de repositórios, conforme representado na figura 1.

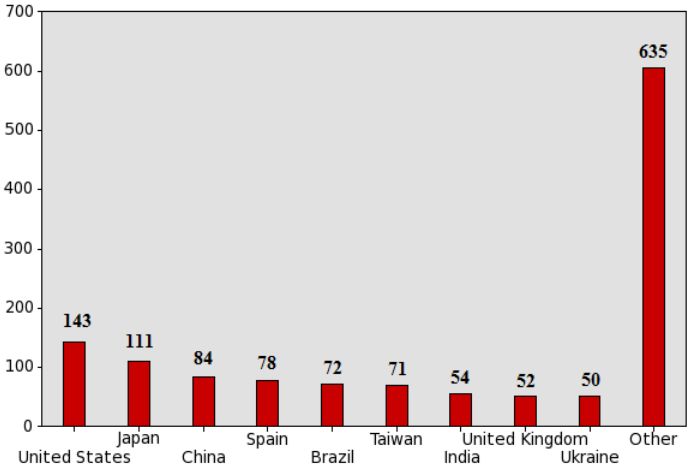

Figura 1 : Número de repositórios digitais com a ferramenta DSpace distribuído por países.

Fonte: ROAR, 2013 (Adaptado).

Desde o desenvolvimento final do DSpace pelo MIT em 2002, o crescimento no número de repositórios digitais se manifesta progressivamente ao longo dos anos em nível mundial. Essa linha da evolução de uso no tempo é reproduzida na figura 2.

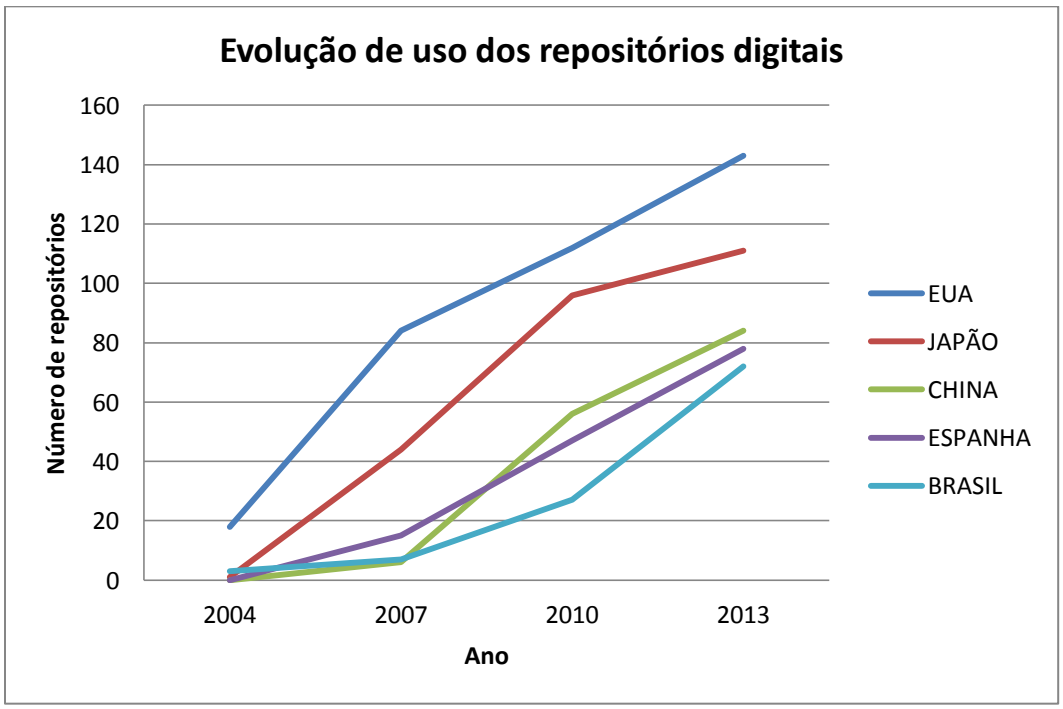

Figura 2 : Evolução de uso no tempo dos repositórios digitais DSpace no Brasil e no mundo.

Fonte: ROAR (2013).

Os países que mais se destacam na implementação de repositórios DSpace são os Estados Unidos, Japão, China, Espanha e Brasil. De acordo com os dados disponíveis no ROAR, o período de maior crescimento no Brasil se revela a partir do ano de 2011. Até o ano de 2010 existiam 27 repositórios no país inseridos na base de dados do ROAR, de 2011 até hoje esse número aumentou em 45, correspondendo a um progresso de 63% na criação de novos repositórios digitais com a ferramenta DSpace.

4 Preservação digital e vulnerabilidades dos repositórios institucionais

Existe uma preocupação universal com a preservação da memória coletiva, cautela justificada pela necessidade de salvaguarda do conhecimento de valor considerável gerado por uma nação. A preservação de documentos digitais é um dos maiores desafios do nosso século, devido aos avanços tecnológicos e ao crescimento da produção de informações em formato digital.

Inicialmente, as técnicas envolvidas com a preservação digital eram baseadas no conceito de identificar medidas que garantissem a vida útil dos arquivos, mas atualmente está relacionada ao conhecimento sobre os métodos de preservação para diminuir os riscos que podem afetar a longevidade do patrimônio informacional.

Todo arquivo está sujeito a riscos e eventuais danos que podem prejudicar o acervo institucional de qualquer organização. Esses acidentes não existem apenas no meio físico, também acontecem no ambiente virtual, e para minimizá-los é necessário adotar estratégias e medidas eficazes para a proteção dos documentos.

> [...] a identificação dos potenciais perigos decorrentes do ambiente digital nos processos de guarda e preservação da memória tem por objetivo permitir, antecipadamente, a adoção de medidas preventivas a fim de eliminar as causas ou reduzir os impactos e consequências dos cenários de acidentes identificados. Assim, a utilização de métodos de análise preliminar de riscos tem por finalidade propor proteção e guarda ao patrimônio informacional gerenciado por sistemas de informação, na eventualidade de um possível acidente. (LIMA; LIMA, 2012, p. 5).

O reconhecimento preliminar das possíveis ameaças inerentes aos conteúdos digitais trazem benefícios às instituições no tocante à administração de recursos financeiros essenciais para a instalação e manutenção de sistemas e processos operacionais. Identificar esses perigos antecipadamente ou possuir o conhecimento necessário para saná-los ou amenizá-los contribui para a gestão eficiente da informação digital.

São diversos os fatores que podem colocar em risco o processo de guarda e acesso da memória digital. Um dos mais comuns diz respeito à obsolescência de hardware e software, pois a tecnologia vive em constante renovação. Interligado a esse aspecto está a utilização de padrões e formatos de arquivos que permitam o amplo acesso e a assistência técnica efetiva para a conversão dos dados nos padrões atuais. Márdero Arellano (2004, p. 16) corrobora essa questão quando afirma que “[...] devem ser usados padrões e converterem-se os documentos nos formatos livres, para que eles sejam acessados após a obsolescência dos equipamentos e programas informáticos em que foram criados”. A despeito da existência destes elementos causadores, estes não são considerados capazes de inutilizar e dificultar o prosseguimento das atividades contínuas dos repositórios institucionais.

Outro ponto importante está relacionado à falta de investimento das próprias instituições, que não disponibilizam os recursos necessários para promover a especialização e o domínio técnico dos profissionais que lidam com a preservação da informação digital, dificultando assim a adaptação desses profissionais ao uso das novas ferramentas de tecnologia. No nível operacional destaca-se a importância de avaliar o funcionamento e a atualização dos repositórios, nesse sentido Targino, Garcia e Paiva (2012) apontam para a constatação de problemas na manutenção dos sistemas dos repositórios digitais, apresentando erros internos, links indisponíveis ou até mesmo inexistentes para o acesso ao conteúdo completo do material.

As ameaças consideradas mais significativas para a preservação digital consistem na falta de gerenciamento dos ativos informacionais, com a ausência de elaboração de normas e manuais estratégicos que orientem quanto ao tratamento de objetos digitais; a falta de políticas de seleção para a preservação da coleção digital e a carência de um controle estatístico com indicadores relevantes para o planejamento, avaliação e gestão do conteúdo armazenado. Essas vulnerabilidades evidenciam “a presença de riscos capazes de causar acréscimo significativo

nos custos e esforços despendidos durante o processo de guarda e preservação por estes RI." (LIMA; LIMA, 2012, p. 11).

As instalações, o acondicionamento e os recursos físicos disponíveis para a conservação dos materiais digitais são indicadores que não se configuram como ameaças expressivas para a preservação e são considerados elementos controláveis nos ambientes dos repositórios institucionais.

O conhecimento desses pontos vulneráveis e da frequência com que eles ocorrem, permite aos gestores anteciparem cuidados e tomarem as providências cabíveis com a preservação e com os custos aplicados durante o processo de armazenamento e acesso de seus acervos informacionais. O exame dessas vulnerabilidades caracteriza uma estratégia relevante na administração das técnicas de preservação digital, conforme a abordagem de Lima e Lima (2012, p. 17)

> Diante destas ameaças, a consciência do perigo se faz cada vez mais necessária, gerando políticas, estratégias e outros instrumentos aplicados a preservação de acervos digitais. Assim, estas medidas surgirão como ferramentas preventivas capazes de reduzir os impactos e consequências dos cenários de acidentes identificados nestes RI.

A preservação de documentos digitais deve adotar políticas e procedimentos documentados que garantam a integridade da informação, disponibilizar o acesso em longo prazo destes documentos para a posteridade, permitir que a informação seja disseminada como reprodução legítima do original e seguir ações imediatas que favoreçam a confiabilidade. Thomaz (2007, p. 88) define que "um repositório digital confiável é mais do que uma organização encarregada de armazenar e administrar objetos digitais".

Um dos atributos dos repositórios digitais confiáveis é a conformidade com o modelo de referência *Open Archival Information System* (OAIS) ou Sistema Aberto para Arquivamento de Informação (SAAI), publicado pelo *Consultive Committee for Space Data Systems*. Outras características como responsabilidade administrativa, sistema de segurança, viabilidade organizacional e adequação financeira completam os requisitos de credibilidade dos arquivos digitais confiáveis. (THOMAZ, 2007). O SAAI é o modelo de preservação de arquivos em longo prazo mais utilizado atualmente. Este modelo deve ser complementado pelas premissas gerais de segurança da informação que devem ser observadas por qualquer organização que se proponha a este tipo de atividade.

5 Segurança da informação

A informação é um insumo de extrema importância na história da humanidade e precisa ser resguardada. Temos ciência que ela esteve presente em todo o período da evolução histórica, desde os primórdios até os tempos atuais. "Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local." (BRASIL, 2007, p. 7). Com a migração da informação para o suporte digital e sua disponibilização pelas redes de computadores este cenário foi alterado.

A informação é um componente representativo na sociedade do conhecimento, a qual surgiu como resultado do fenômeno conhecido como explosão informacional, distinguida pelo aumento quantitativo e acelerado nos processos de produção e disseminação da informação.

Na atual sociedade da informação, ao mesmo passo em que as informações são caracterizadas como a herança fundamental de uma organização, simultaneamente estão vulneráveis a riscos contínuos e a sofrerem perigosas consequências, como nunca estiveram anteriormente. Dessa forma, a segurança da informação traduz-se como um tema categórico para a sobrevivência das instituições. (BRASIL, 2007).

O recurso informacional é um bem precioso para pessoas, empresas, organizações e instituições, constituindo uma mercadoria indispensável principalmente para o processo de tomada de decisões. Nesse contexto, Sêmola (2003 apud MAIA, 2010) afirma que há uma necessidade imprescindível de assegurar e proteger esses ativos informacionais contra acessos de pessoas não autorizadas, alterações ou usos indevidos, como também sua indisponibilidade.

A NBR ISO/IEC 17799 é uma norma de Tecnologia da Informação e Técnicas de Segurança. A versão original foi publicada em 2002 pela Associação Brasileira de Normas Técnicas – ABNT e revisada em 2005 pela *International Standards Organization* – ISO (Organização Internacional de Padrões) e pela *International Electrotechnical Commission* – IEC (Comissão Eletrotécnica Internacional) e passou a ser identificada como NBR ISO/IEC 27002.

A segurança da informação tem a função de proteger a informação de inúmeras formas de ameaças. Para complementar esse processo de resguarda, a segurança da informação pode ser sistematizada em uma tríade de fundamentos básicos: confidencialidade, integridade e disponibilidade. Conforme destacado na NBR ISO/IEC 27002,

> A segurança da informação é aqui caracterizada pela preservação de: a) confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso; b) integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento; c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2002, p. 2).

Na visão de Campos (2006, p. 6 apud MAIA, 2010, p. 11-12) define-se que

> O princípio da confidencialidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação. O princípio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto, confiável. O princípio da disponibilidade é respeitado quando a informação está acessível, por pessoas autorizadas, sempre que necessário.

Outros fatores de preservação como responsabilidade, autenticidade e confiabilidade também podem estar presentes e envolvidos no processo da segurança da informação. Um episódio isolado ou uma série de eventos indesejados podem acarretar em incidentes imprevistos para a segurança da informação e apresentam uma ampla probabilidade de ameaça para o sistema, ocasionando o comprometimento da segurança dos dados.

Muitos sistemas de informação e redes de computadores de instituições não foram projetados para serem ambientes seguros. O acesso pode ser comprometido por diversos tipos de ameaças existentes à segurança da informação e os ataques são oriundos de várias fontes como invasão de hackers, fraudes eletrônicas, sabotagens por vírus, vandalismo e até mesmo como alvo de espionagem governamental.

6 Desenvolvimento e procedimentos metodológicos

Esta pesquisa caracteriza-se como descritiva e quantitativa e serão abordadas considerações a respeito dos métodos utilizados para a coleta e análise dos dados. A abordagem quantitativa apresenta como característica a análise numérica dos dados coletados por meio de procedimentos estatísticos, representados graficamente em quadros e ilustrações.

O universo abrangido pelo estudo são as Universidades Federais do Brasil, composto por 59 instituições acadêmicas conforme consta no endereço eletrônico do MEC[4]. A amostra corresponde a 30 (trinta) universidades federais de todas as regiões do país que possuem Repositórios Digitais de Acesso Aberto em sua esfera acadêmica (quadro1).

A técnica adotada para a coleta e análise dos dados consistiu na execução de Testes de Penetração nos sistemas dos repositórios, através da ferramenta Netsparker. Esses testes podem ser considerados como “instrumentos utilizados com a finalidade de obter dados que permitam medir o rendimento, a frequência, a capacidade ou a conduta de indivíduos [ou organismos], de forma quantitativa”. (MARKONI; LAKATOS, 2003, p. 223).

O Netsparker é um software de escaneamento de segurança que executa *Penetration Test* (Teste de Penetração, tradução nossa) em sites e detecta automaticamente as falhas que poderiam deixá-los perigosamente expostos. Segundo Assunção (2010, p. 93), “um dos ataques mais comuns hoje é a injeção de comandos SQL (Structured Query Language). [...] SQL é um banco de dados muito utilizado atualmente, que possui várias versões [...]”.

A ferramenta Netsparker está apta a identificar muitas vulnerabilidades de segurança da Web no decorrer da varredura do sistema, sendo capaz de explorar habilmente as falhas de injeção de comandos SQL em diferentes bancos de dados com alta precisão.

O Teste de Penetração permite identificar potenciais vazamentos de informação que podem prejudicar um organismo ou empresa, e compreende fases que abrangem desde uma abertura na segurança por um ataque externo e/ou interno até o acesso indevido a dados confidenciais não autorizados, eventos que podem causar danos irreparáveis aos sistemas. Conforme Assunção (2010, p. 55), o objetivo deste teste é detectar falhas através de simulações de ataques e invasões a um sistema, rede ou ambiente no qual se analisar.

Os testes foram realizados em laboratório na Universidade Federal da Paraíba, no período de 18/06/2013 a 16/07/2013. A relação dos repositórios digitais federais pode ser encontrada no diretório do IBICT[5].

Algumas dificuldades foram identificadas no decorrer da fase dos testes de vulnerabilidades dos repositórios digitais, as quais são relatadas a seguir:

- Os endereços dos repositórios da UFAC, UFF, UFJF e UNIFESP apresentaram falha no carregamento da página e não foi possível ter acesso ao seu conteúdo, o que impossibilitou a execução do teste;
- O repositório da UFPE exibiu um endereço não localizado e também não foi possível testar seu desempenho;
- Nos repositórios da UFAL, UFGD, UFRGS, UFVJM e UFV os testes de vulnerabilidade não foram concluídos, pois em determinado ponto a velocidade de escaneamento chegava a zero e o andamento da varredura era prejudicado até cessar por completo;
- Houve a necessidade de refazer a análise de risco do repositório da UNB devido a uma divergência na verificação dos resultados. O primeiro teste foi realizado em 19/06/2013 e o segundo em 12/08/2013.

Portanto, das 30 (trinta) instituições federais consideradas na amostra, 20 (vinte) foram analisadas com sucesso, o que corresponde a aproximadamente 67% dos repositórios digitais testados. A quadro abaixo apresenta o histórico do desenvolvimento da análise de risco dos repositórios institucionais federais:

Quadro 1: Histórico da análise de risco dos Repositórios Institucionais Federais (continua).

Nº	Instituições	Repositório	Data de consulta	Tempo de escaneamento
1	UFAC	http://repositorios.ufac.br:8080/repositorio/	Sem acesso	
2	UFAL	http://www.repositorio.ufal.br/	Teste não concluído	
3	UFBA	https://repositorio.ufba.br/ri/	23/06/2013	54min
4	UnB	http://repositorio.bce.unb.br/	12/08/2013	1h33min
5	UFC	http://www.repositorio.ufc.br:8080/ri/	28/06/2013	1h04min
6	UFES	http://repositorio.ufes.br/	27/06/2013	1h20min
7	UFF	http://repositorio.uff.br/jspui/	Sem acesso	
8	UFG	http://repositorio.bc.ufg.br/	28/06/2013	57min
9	UFGD	http://www.ufgd.edu.br:8080/jspui/	Teste não concluído	
10	UFJF	http://repositorio.ufjf.br:8080/jspui/	Sem acesso	

Fonte: Dados da pesquisa (2013)

Quadro 1: Histórico da análise de risco dos Repositórios Institucionais Federais (conclusão).

Nº	Instituições	Repositório	Data de consulta	Tempo de escaneamento
11	UFLA	http://repositorio.ufla.br/	10/07/2013	3h04min
12	UFMA	http://www.repositorio.ufma.br:8080/jspui/	26/06/2013	2h52min
13	UFMS	http://repositorio.cbc.ufms.br:8080/jspui/	15/07/2013	1h31min
14	UFMG	https://dspaceprod02.grude.ufmg.br/dspace/	18/06/2013	12min
15	UFOP	http://www.repositorio.ufop.br/	30/06/2013	1h29min
16	UFPA	http://repositorio.ufpa.br/jspui/	27/06/2013	2h09min
17	UFPB	http://rei.biblioteca.ufpb.br/jspui/	22/06/2013	2h24min
18	UFPR	http://dspace.c3sl.ufpr.br:8080/dspace/	30/06/2013	5h45min
19	UFPEL	http://guaiaca.ufpel.edu.br:8080/jspui/	16/07/2013	3h25min
20	UFPE	http://www.repositorios.ufpe.br/jspui/	Não localizado	
21	FURG	http://repositorio.furg.br:8080/jspui/	01/07/2013	2h03min
22	UFRGS	http://www.lume.ufrgs.br/	Teste não concluído	
23	UFRN	http://repositorio.ufrn.br:8080/jspui/	18/06/2013	1h36min
24	UFSC	http://repositorio.ufsc.br/	18/06/2013	3h38min
25	UFSCAR	http://livresaber.sead.ufscar.br:8080/jspui/	06/07/2013	2h18min
26	UNIFESP	http://200.133.202.157:8080/jspui/	Sem acesso	
27	UFS	https://ri.ufs.br/	08/07/2013	1h34min
28	UFU	http://repositorio.ufu.br/	08/07/2013	2h20min
29	UFVJM	http://acervo.ufvjm.edu.br:8080/jspui/	Teste não concluído	
30	UFV	http://riserver.cpd.ufv.br:8080/repositorio/	Teste não concluído	

Fonte: Dados da pesquisa (2013)

Como qualquer base de dados, os repositórios digitais estão vulneráveis a diversos tipos de ameaças. Essas vulnerabilidades podem colocar em risco seu funcionamento e expor o repositório a ataques externos. A ferramenta de análise de segurança utilizada para testar os repositórios institucionais federais detecta e identifica falhas que podem expor perigosamente o sistema a ataques. Contudo não prejudica ou explora as falhas encontradas.

A descrição dos testes e as definições das vulnerabilidades empregadas nesta pesquisa são traduções dos manuais do software Netsparker e estão em conformidade com iniciativas criadas por diferentes organizações que se empenham em classificar as vulnerabilidades encontradas nos sistemas e que podem prejudicar a segurança da informação. O quadro seguinte indica a relação das classificações aplicadas:

Quadro 2: Relação de organizações que monitoram e classificam os tipos de vulnerabilidades em sistemas na Web.

Organização	Relação
WASC – *Web Application Security Consortium* (Consórcio de Segurança de Aplicações Web)	Esforço cooperativo para esclarecer e organizar as ameaças à segurança de uma página na Internet.
OWASP – *Open Web Application Security Project* (Projeto de Segurança de Aplicações Web Abertas)	Comunidade aberta dedicada a capacitar as organizações para conceber, desenvolver, adquirir, operar e manter aplicações que podem ser confiáveis.
CWE – *Common Weakness Enumeration* (Enumeração de Fraquezas Comuns)	Lista os tipos de fraquezas de software desenvolvidas por iniciativas da comunidade voltada para desenvolvedores e profissionais de segurança.
CAPEC – *Common Attack Pattern Enumeration and Classification* (Ataque Comum Padrão de Enumeração e Classificação)	A comunidade disponibiliza fontes de conhecimento para a construção de um software seguro.
PCI – *Payment Card Industry*	Apresenta um Padrão de Segurança de Dados, com requisitos e procedimentos de avaliação de segurança.

Fonte: Dados da pesquisa (2013).

Os riscos são divididos em cinco níveis: crítico, alto, médio, baixo e alerta. Para efeito desta pesquisa a análise dos conceitos referentes aos alertas foram desconsiderados. Conforme verificação dos resultados apurados foi identificada um única vulnerabilidade de risco classificado como crítico:

- *Boolean Based SQL Injection* – a injeção SQL ocorre quando a entrada de dados, por exemplo, um usuário, é interpretado como um comando SQL, em vez de dados normais. Essa é uma vulnerabilidade muito comum e a sua exploração bem sucedida pode ter implicações importantes. A vulnerabilidade foi confirmada por meio da execução de um teste de consultas SQL no banco de dados. Nesses testes, o SQL Injection não era óbvio, mas as diferentes respostas da página com base no teste de injeção permitiu identificar e confirmar o SQL Injection.

A análise de segurança detectou os seguintes tipos de vulnerabilidades de alto risco:

- *Password Transmitted over HTTP* – identifica que dados de senha são enviados através de HTTP. Um atacante acessando o site do repositório pode realizar uma invasão para capturar a senha do usuário.
- *Cross-site Scripting (XSS)* – permite a um invasor executar um script dinâmico no contexto da aplicação. Isso dá lugar a variadas e diferentes oportunidades de ataque, principalmente o sequestro da sessão atual do usuário ou alteração da aparência da página, modificando o código HTML na hora de roubar as credenciais do usuário. XSS tem como alvo os usuários do aplicativo em vez do servidor. Embora esta seja uma limitação, uma vez que permite que atacantes sequestrem a sessão de outros usuários, um invasor pode atacar um administrador para obter o controle total sobre a aplicação.
- *SVN Detected* – detecta arquivos divulgados pelo código de sistemas de controle de versão de origem, como CVS, GIT e SVN. Um invasor pode explorar este problema para ter acesso ao código-fonte da aplicação, ou pode recuperar a configuração e/ou outros arquivos importantes.
- *Cookie Not Marked as Secure* – identificou um cookie não marcado como seguro e transmitido através de HTTPS. Isso significa que o cookie poderia ser roubado por um invasor que pode interceptar e decifrar com sucesso o tráfego, ou após um bem sucedido ataque man-in-the-middle (homem no meio). Nesse tipo de

ataque, o computador do invasor age como um servidor para o usuário, capturando e descriptografando os dados através de uma chave privada de certificado, tornando a criptografá-los e enviando-os para o servidor remoto no papel de cliente. (ASSUNÇÃO, 2010).

As vulnerabilidades de risco médio identificadas foram:

- *HTTP Header Injection* – detecta problemas de injeção de cabeçalho em aplicações web que podem causar sérios problemas. O mais comum deles são Cross-site Scripting e sequestro de sessão, tomando a forma de ataques de fixação de sessão.
- *Insecure Transportation Security Protocol Supported (SSLv2)* – detecta que o servidor web está configurado para suportar a comunicação segura através de um protocolo de transporte inseguro (SSLv2), que possui várias falhas. O tráfego seguro do site pode ser observado quando foi estabelecido sobre este protocolo. Os atacantes podem realizar ataques e observar o tráfego de criptografia entre o site e os visitantes.
- *Weak Ciphers Enabled* – detecta que o servidor web está configurado para permitir o uso de cifras fracas durante a comunicação segura (SSL). Invasores podem montar ataques de força bruta para decifrar a comunicação segura entre o servidor e os visitantes.
- *Invalid SSL Certificate* – verifica que o servidor web utiliza um certificado SSL inválido. Um certificado SSL pode ser criado e assinado por qualquer um. É necessário ter um certificado SSL válido para fazer com que os visitantes tenham certeza sobre a comunicação segura entre o site e eles. Se o site tiver um certificado inválido, os visitantes vão ter dificuldade em distinguir entre seu certificado e os de atacantes.

Os tipos de vulnerabilidades de baixo risco encontrados foram:

- *Cookie Not Marked as HttpOnly* – relata que um cookie não foi marcado como HTTPOnly. Cookies HTTPOnly não podem ser lidos pelos scripts do lado do usuário, portanto, marcar um cookie como HTTPOnly pode fornecer uma camada adicional de proteção contra ataques de Cross-site Scripting.
- *Internal Server Error* – O servidor respondeu com um status HTTP 500. Isto indica que há um erro do servidor. As razões podem variar, o comportamento deve ser cuidadosamente analisado.
- *Auto Complete Enabled* – a função Auto Completar foi ativada em um ou mais campos de formulário sensíveis, como senhas. Os dados inseridos nesses campos serão armazenados em cache pelo navegador. Um invasor que pode acessar o computador da vítima poderia roubar esta informação. Isto é especialmente importante se o aplicativo é comumente usado em computadores públicos.
- *Version Disclosure (Apache)* – identifica uma versão divulgação (Apache), em resposta HTTP do servidor web de destino. Essas informações podem ajudar a um atacante obter uma maior compreensão dos sistemas em uso e, potencialmente, desenvolver novos ataques direcionados a versão específica do Apache.
- *Version Disclosure (Apache Coyote)* – determina que o servidor web de destino está divulgando a versão Coyote Apache em sua resposta HTTP. Um atacante pode usar as informações divulgadas para colher as vulnerabilidades de segurança específicas para a versão identificada.
- *Version Disclosure (Tomcat)* – identifica que o servidor web alvo está divulgando a versão Tomcat em sua resposta HTTP. Essas informações podem ajudar a um atacante obter uma maior compreensão dos sistemas em uso e, potencialmente, desenvolver novos ataques direcionados à versão específica do Tomcat.
- *Exception Report Disclosure (Tomcat)* – determina que o servidor web alvo está divulgando os dados do relatório de exceção na resposta HTTP. Um atacante pode obter informações como o caminho de arquivo físico dos arquivos do Tomcat e se concentrar potencialmente no desenvolvimento de novos ataques ao sistema de destino.
- *Social Security Number Disclosure* – identifica Números de Segurança Social (SSN) no site. Números de Segurança Social tem sido usados por atacantes no roubo de identidade já que muitas organizações,

incluindo empresas, agências governamentais, hospitais e instituições de ensino utilizam o SSN como o identificador primário para os seus sistemas de manutenção de registros.

As vulnerabilidades identificadas nas verificações de segurança dos repositórios digitais foram organizadas e distribuídas por tipos e classificadas nos 5 (cinco) níveis de risco: crítico, alto, médio, baixo e alertas. A Quadro 3 apresenta os resultados por tipos de vulnerabilidades detectadas nos ambientes computacionais dos repositórios analisados.

Quadro 3: Tipos de vulnerabilidades identificados nos Repositórios Institucionais Federais (continua).

Nível	Tipo de vulnerabilidade	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10	U11	U12	U13	U14	U15	U16	U17	U18	U19	U20
Crítico	Boolean Based SQL Injection				1																
Alto	Password Transmitted over HTTP	1		1	1	1		1	1	1	1	1	1		1	1	1		1	1	1
	XSS (Cross-site Scripting)				150					4		32				1	1	28		27	
	SVN Detected																	1			
	Cookie Not Marked as Secure																	1			
Médio	HTTP Header Injection				8	30						35									
	Insecure Transportation Security Protocol Supported (SSLv2)		1																		
	Weak Ciphers Enabled		1																		
	Invalid SSL Certificate									1											

Fonte: Dados da pesquisa (2013).

Quadro 3: Tipos de vulnerabilidades identificados nos Repositórios Institucionais Federais (conclusão).

Nível	Tipo de vulnerabilidade	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10	U11	U12	U13	U14	U15	U16	U17	U18	U19	U20
Baixo	Cookie Not Marked as HttpOnly	1	1		1				1					1		1	1	1	1		1
	Internal Server Error	1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Auto Complete Enabled	1		1	1	1	1	1	1	1	1	1	1		1	1	1	1	1	1	1
	Version Disclosure (Apache)																	1			
	Version Disclosure (Apache Coyote)	1		1			1	1	1	1	1		1	1	1	1		1	1	1	1
	Version Disclosure (Tomcat)	1							1			1				1	1	1	1		1
	Exception Report Disclosure (Tomcat)	1							1										1		
	Social Security Number Disclosure									1											

Fonte: Dados da pesquisa (2013).

7 Recomendações para a segurança e considerações finais

Estar seguro é uma necessidade, reforçada quando se trabalha no mundo tecnológico. É importante definir medidas que promovam a proteção e permitam o funcionamento eficaz dos serviços prestados em caso de comprometimento do sistema ocasionado pelas falhas na segurança.

Para proteger os ativos informacionais de uma instituição é necessário combinar ações preventivas e de recuperação, que consistem em um conjunto de técnicas e procedimentos que devem ser adotados para a segurança digital. “Essas estratégias e procedimentos deverão minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.” (BRASIL, 2007, p. 33).

As normas e ferramentas de análise de segurança indicam procedimentos e oferecem informações para incrementar as medidas de segurança. Por exemplo, um método reconhecido para atenuar a ameaça de vulnerabilidades baseadas em injeções de comando SQL é a utilização de consultas parametrizadas para a filtragem dos caracteres digitados, impedindo a inserção de comandos pelo invasor nos scripts dos programas.

Outra recomendação é para evitar que senhas de usuários sejam capturadas: todos os dados sensíveis devem ser transferidos via HTTPS em vez de HTTP. Os formulários devem ser servidos por HTTPS e todos os aspectos da aplicação que aceitam entrada do usuário a partir do processo de login só devem ser fornecidos por HTTPS.

Para impedir ataques XSS é altamente recomendado o uso de uma biblioteca de codificação, pois a mesma é de grande complexidade. Dessa forma evita-se que atacantes utilizem essa técnica para obter acesso aos cookies de usuários sem autorização, através do navegador.

Ameaças sempre vão existir e falhas sempre vão ocorrer, independente dos recursos investidos em software, hardware e pessoal capacitado. Executar Testes de Penetração, bem como efetuar a varredura do sistema com scanners de vulnerabilidades e realizar pesquisas manuais são recomendações bastante úteis para prevenção e correção dos problemas apontados. (ASSUNÇÃO, 2010).

A implementação de uma política de segurança, o uso de controles de acesso aos recursos de processamento e a aplicação de tecnologias voltadas para a segurança de serviços de redes de computadores como autenticação, certificados de segurança válidos, encriptação de dados, dentre outros, são medidas que restringem o acesso a quem de direito e tornam o ambiente menos suscetível a invasões. Também é indispensável o uso de softwares como antivírus, firewall e monitoradores do sistema, que auxiliam na segurança.

Os sistemas digitais estão vulneráveis a todo tipo de riscos, sejam eles desastres naturais, acidentes ou ataques intencionais, o que resulta no acontecimento de situações imprevistas. As falhas na segurança podem causar impactos inesperados nas redes de computadores de uma instituição, e os resultados dessas lacunas abrangem desde ocorrências de baixa relevância até fatos de consequências calamitosas para a organização.

Com a disponibilidade e utilização das ferramentas tecnológicas, a informação é transmitida com muito mais facilidade e presteza por todo o mundo. O processamento instantâneo da informação por meio da Internet promoveu sua difusão em larga escala. Desse modo, os dados informacionais passaram a apresentar uma maior necessidade de segurança para sua salvaguarda, independente do suporte utilizado.

Nesta pesquisa foram distinguidos os aspectos essenciais da segurança da informação, as vulnerabilidades mais comuns e as medidas adotadas para uma melhor segurança dos dados, bem como os resultados da aplicabilidade dos testes nos sistemas gerenciadores dos repositórios digitais.

Para que seja efetuada a prestação de bons serviços em ambientes informatizados é indispensável a aplicação de boas práticas para segurança da informação, visando a proteção do patrimônio intelectual da estrutura organizacional. Para tanto, é essencial a colaboração de todos que interagem com o sistema, englobando profissionais da área, gestores, funcionários e usuários.

Conforme a análise dos dados resultantes das aplicações dos testes permitiram uma apreciação pormenorizada das ameaças concernentes à segurança dos ativos informacionais depositados nos repositórios digitais, quantificando e denominando os riscos encontrados, assim como possibilitou diferenciar os elementos causadores das falhas e apontou a adoção de técnicas e procedimentos adequados que podem contribuir para a preservação dos dados digitais.

Considerando os resultados verificados na pesquisa, pode-se concluir que o desempenho dos repositórios digitais das IES federais ainda não está completamente satisfatório em relação à Segurança da Informação. Como apresentado no desenvolvimento do trabalho, no quesito correspondente ao acesso das informações dos usuários, 80% dos repositórios testados está exposto à vulnerabilidade de alto risco *Password Transmitted over HTTP*, ou seja, a recuperação da senha pessoal por meio de ataques simples. E no que diz respeito às vulnerabilidades de baixo risco, os destaques se concentram no item de Erro Interno do Servidor, encontrado em 95% dos testes e na função de Auto Completar, responsável por facilitar a recuperação de informações sigilosas em 90% dos repositórios.

Quando analisados em conjuntos com os resultados apresentados por Lima e Lima(2012), verifica-se que os ambientes destes repositórios digitais são muito frágeis, e não possuem os requisitos para preservar a informação neles armazenadas, como proposto. Por fim, convém evidenciar a relevância da aplicação das práticas de segurança recomendadas pelas normas vigentes e por profissionais qualificados, com o intuito de suprir necessidades básicas para a preservação dos dados e diminuir a suscetibilidade de invasão ou quaisquer outros tipos de ameaças a que estão expostos os repositórios digitais de uma instituição.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:** Tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2002.

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do hacker ético**. 3. ed. Florianópolis: Visual Books, 2010.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação.** 2. ed. Brasília, DF, 2007. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF>. Acesso em: 24 ago. 2013.

CAPEC. Common Attack Pattern Enumeration and Classification. Disponível em: <http://capec.mitre.org/index.html>. Acesso em: 28 out. 2013.

CWE. Common Weakness Enumeration. Disponível em: <http://cwe.mitre.org/about/index.html>. Acesso em: 28 out. 2013.

FACHIN, Geisy Regina Bories, et al. Gestão do conhecimento e a visão cognitiva dos repositórios institucionais. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 14, n. 2, p. 220-236, maio./ago. 2009. Disponível em: <http://www.scielo.br/pdf/pci/v14n2/v14n2a15.pdf>. Acesso em: 15 maio 2013.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Editora Atlas, 2002.

KURAMOTO, Hélio. Informação científica: proposta de um novo modelo para o Brasil. **Ciência da Informação**, Brasília, v. 35, n. 2, p. 91-102, maio/ago. 2006. Disponível em: <http://www.scielo.br/pdf/ci/v35n2/a10v35n2.pdf>. Acesso em: 09 maio 2013.

KURAMOTO, Hélio. Réplica - Acesso Livre: caminho para maximizar a visibilidade da pesquisa. **RAC**, Curitiba, v. 12, n. 3, p. 861-872, jul./set. 2008. Disponível em: <http://www.scielo.br/pdf/rac/v12n3/13.pdf>. Acesso em: 09 maio 2013.

LIMA, Fanny do Couto Ribeiro de; LIMA, Marcos Galindo de. Preservação digital da informação científica: uma análise de risco em repositórios institucionais brasileiros. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 13., 2012, Rio de Janeiro. **Anais eletrônicos...** Disponível em: <http://www.eventosecongressos.com.br/metodo/enancib2012/arearestrita/pdfs/19495.pdf>. Acesso em: 01 jun. 2013.

MAIA, Ana Maria Rocha. **Segurança da informação:** estudo para implantação do arquivo da Seplan. 2010. 57 f. Trabalho de Conclusão de Curso (Graduação em Biblioteconomia)–Universidade Federal do Rio Grande do Norte, Natal, 2010. Disponível em: <http://repositorio.ufrn.br:8080/monografias/handle/1/178>. Acesso em 24 ago. 2013.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Editora Atlas, 2003.

MÁRDERO ARELLANO, Miguel Angel. Preservação de documentos digitais. **Ciência da Informação**, Brasília, v.33, n.2, p. 15-27, maio/ago. 2004. Disponível em: <http://www.scielo.br/pdf/ci/v33n2/a02v33n2.pdf>. Acesso em: 10 maio 2013.

OLIVEIRA, Renan Rodrigues de; CARVALHO, Cedric Luiz de. **Bibliotecas Digitais e o Repositório Fedora**. Instituto de Informática. Universidade Federal de Goiás, 2011. Disponível em: <http://www.inf.ufg.br/sites/default/files/uploads/relatorios-tecnicos/RT-INF_002-11.pdf>. Acesso em: 19 maio 2013.

OWASP. Open Web Application Security Project. Disponível em: <https://www.owasp.org/index.php/Main_Page>. Acesso em: 28 out. 2013.

PCI. Payment Card Industry. Disponível em: <https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf>. Acesso em: 28 out. 2013.

RIBEIRO, O. B ; VIDOTTI, S. A. B. G. Otimização do acesso à informação científica: discussão sobre a aplicação de elementos da arquitetura da informação em repositórios digitais. **Biblos**, Rio Grande, v. 23, n. 2, p. 105-116, 2009. Disponível em: <http://www.seer.furg.br/biblos/article/view/1309/593>. Acesso em: 10 maio 2013.

TARGINO, Maria das Graças; GARCIA, Joana Coeli Ribeiro; PAIVA, Maria José Rodrigues. Repositórios institucionais brasileiros: entre o sonho e a realidade. In: CONFERENCIA INTERNACIONAL ACCESO ABIERTO, COMUNICACIÓN CIENTÍFICA Y PRESERVACIÓN DIGITAL, 1., 2012, Barranquilla, Colombia. **Anais Eletrônicos...** Disponível em: <http://eventos.uninorte.edu.co/index.php/biredial/biredial2012/paper/view/360>. Acesso em: 02 jun. 2013.

THOMAZ, Kátia P. Repositórios digitais confiáveis e certificação. **Arquivística.net**, Rio de Janeiro, v. 3, n. 1, p. 80-89, jan./jun. 2007. Disponível em: <http://www.brapci.ufpr.br/documento.php?dd0=0000004775&dd1=ac3d4>. Acesso em: 03 jun. 2013.

VIANA, Cassandra Lúcia de Maya; MÁRDERO ARELLANO, Miguel Angel. *Repositórios institucionais baseados em DSpace e EPrints e sua viabilidade nas instituições acadêmico-científicas*. In: SEMINÁRIO NACIONAL DE BIBLIOTECAS UNIVERSITÁRIAS, 14., 2006, Salvador. **Anais eletrônicos...** Disponível em: <http://eprints.rclis.org/8834/>. Acesso em: 13 maio 2013.

VIANA, Cassandra Lúcia de Maya; MÁRDERO ARELLANO, Miguel Angel; SHINTAKU, Milton. *Repositórios institucionais em ciência e tecnologia: uma experiência de customizacão do DSpace*. In: SIMPOSIO INTERNACIONAL DE BIBLIOTECAS DIGITAIS, 3., 2005, São Paulo. **Anais eletrônicos...** Disponível em: <http://eprints.rclis.org/7168/>. Acesso em: 12 maio 2013.

WASC. Web Application Security Consortium. Disponível em: <http://projects.webappsec.org/w/page/13246927/FrontPage>. Acesso em: 28 out. 2013.

WEITZEL, Simone da Rocha. O papel dos repositórios institucionais e temáticos na estrutura da produção científica. **Em Questão**, Porto Alegre, v. 12, n. 1, p. 51-71, jan./jun. 2006. Disponível em: <http://seer.ufrgs.br/EmQuestao/article/view/19/7>. Acesso em: 14 maio 2013.

WEITZEL, Simone da Rocha. Reflexões sobre os repositórios institucionais. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 29., 2006, Brasília. **Anais eletrônicos...** Disponível em: <http://eprints.rclis.org/8744/1/reflexoes_weitzel_endocom.pdf>. Acesso em: 15 maio 2013.

Notas

[1]Disponível em: <http://www.brapci.ufpr.br/indicador_producao.php>. Acesso em: 17 out 2013.

[2]O conceito na íntegra está disponível em: <http://www.ibict.br/informacao-para-ciencia-tecnologia-e-inovacao%20/repositorios-digitais>. Acesso em: maio 2013.

[3]Website: http://roar.eprints.org/

4Informações disponíveis em: <http://emec.mec.gov.br/>. Acesso em: 17 out. 2013.

5Disponível em: <http://diretorio.ibict.br/handle/1/4/browse?type=title&submit_browse=Title>.

Dados dos autores

Valdete Fernandes Belarmino

Possui graduação em Biblioteconomia pela Universidade Federal da Paraíba (2014) . Tem experiência na área de Ciência da Informação, com ênfase em Biblioteconomia.

valdete.fb@gmail.com

Wagner Junqueira de Araújo

Doutor em Ciência da Informação pela Universidade de Brasília, Mestre em Ciência da Informação pela Universidade de Brasília, Graduado em Ciência da Computação. Professor do Programa de Pós-Graduação em Ciência da Informação – UFPB. Professor Adjunto do Departamento de Ciência da Informação da Universidade Federal da Paraíba-UFPB.

wagnerjunqueira.araujo@gmail.com

Recebido - Received : 2014-02-15

Aceitado - Accepted : 2014-09-30