RDBCI: Revista Digital Biblioteconomia e Ciência da Informação
RDBCI : Digital Journal of Library and Information Science

10.20396/rdbci.v0i0.8646416

SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS UNIVERSITÁRIAS: A ATUAÇÃO DO BIBLIOTECÁRIO NO PLANEJAMENTO E NA IMPLANTAÇÃO DE NOVAS POLÍTICAS INSTITUCIONAIS

INFORMATION SECURITY IN ACADEMIC LIBRARIES: THE ROLE OF THE LIBRARIAN IN PLANNING AND INTRODUCING NEW INSTITUTIONAL POLICIES

SEGURIDAD DE LA INFORMACIÓN EN BIBLIOTECAS DE UNIVERSIDAD: LA INTERPRETACIÓN DEL BIBLIOTECARIO EN LA PROYECCIÓN Y EN LA INTRODUCCIÓN DE NUEVA POLÍTICA INSTITUCIONAL

Juliana Soares Lima[1], Ana Rafaela Sales de Araújo, Francisco Edvander Pires Santos, Luiz Gonzaga Mota Barbosa, Izabel Lima dos Santos
[1]Universidade Federal do Ceará

Correspondência

[1]Juliana Soares Lima
Universidade Federal do Ceará
Fortaleza, CE.
E-mail: juliana.lima@ufc.br
ORCID: http://orcid.org/0000-0001-9399-673X

Submetido em: 31-08-2016
Aceito em: 17-01-2017
Publicado: 20-03-2017

JITA: LH. Computer and network security.

RESUMO: Apresenta uma discussão sobre a atuação do bibliotecário como um profissional importante no planejamento, na elaboração e na implantação de uma Política de Segurança da Informação em Bibliotecas Universitárias, trabalhando em conjunto com os profissionais da área de Tecnologia da Informação. Discorre acerca das principais pragas virtuais existentes que tendem a infectar os computadores das bibliotecas. Ratifica, tendo como base a legislação vigente e documentos normativos, a importância do bibliotecário estar inserido nas principais tomadas de decisão referentes à segurança da informação, tais como o planejamento de uma Política de Segurança da Informação consistente e que supra as necessidades das Bibliotecas Universitárias como instituições propensas a ataques virtuais. Expõe, com base nos resultados alcançados por meio de pesquisa-ação, os principais tópicos e diretrizes que devem constar numa Política de Segurança da Informação, tendo em vista os problemas encontrados nos computadores das bibliotecas e a análise de conteúdo de relatórios elaborados a partir do preenchimento de formulários nas visitas. Conclui que Política de Segurança da Informação deve ser validada pela gestão e pelos setores competentes dos departamentos e/ou divisões aos quais as Bibliotecas Universitárias estejam hierarquicamente subordinadas.

PALAVRAS-CHAVE: Segurança da informação. Biblioteca universitária. Políticas de segurança.

ABSTRACT: This study presents a short discussion about the role of the librarian as a mediator at planning, developing and implementing an Information Security Policy in Academic Libraries, by working together with professionals in the field of Information Technology. It also discusses the main virtual threats and some risks that are prone to infect computers in libraries. Based on the current legislation and on some normative documents about information security, it is confirmed the importance of the librarian take part in the main decision-making related to information security, such as planning a consistent Information Security Policy which be able to see the specific needs of Academic Libraries as institutions prone to cyberattacks. The main topics and guidelines to carry out an Information Security Policy are presented based on the results that were obtained through an action research, by visiting libraries to fill in application forms and to compose reports whose content was analyzed. Finally, the study concludes that Information Security Policy must be validated by managers of sectors or departments which the Academic Library is hierarchically subordinate to.

KEYWORDS: Information security. Academic libraries. Security policies.

RESUMEN: Presenta una discusión sobre la actuación del bibliotecario como un profesional importante para la planificación, desarollo y la implatación de una Política de Seguridad de la Información en Bibliotecas de Universidades, que trabajan en conjunto con profesionales en el campo de la Tecnología de la Información. Habla sobre las principales amenazas virtuales existentes que proponem infectar los ordenadores en las bibliotecas. Teniendo por base la legislación corriente y los documentos normativos, la importancia del bibliotecario és introducida en las principales tomas de decisiones relacionada con la seguridad de información, como la planificación de una Política de Seguridad de la Información consistente y que suple las necesidades de las Bibliotecas de Universidades como instituciones propensas a los ataques virtuales. Con base en los resultados alcanzados a través de invertigación-acción, expone los principales temas y reglas que deben mostrarse en una Política de Seguridad de la Información, visando los problemas encontrados en los ordenadores de las bibliotecas y análisis de los contenidos de informes elaborados, seguidos de formularios llenados en invitaciones. Concluye que la Política de Seguridad de la Información debe ser validada por la dirección y los sectores relevantes de los departamentos y divisiones los cuales las Bibliotecas de Universidades son jerárquicamente subordinadas.

PALABRAS LLAVE: Seguridad de la información. Bibliotecas académicas. Políticas de seguridad.

1 INTRODUÇÃO

Satisfazer as necessidades informacionais de cada usuário, individualmente, é importante tanto na forma tradicional de atendimento (presencialmente) quanto na forma que vem sendo exigida (virtualmente) no cotidiano das Bibliotecas Universitárias (BUs). Para tanto, controlar e reduzir incidentes tecnológicos e de segurança, dentre outros fatores, torna-se extremamente importante com a finalidade de assegurar a operação da rede em níveis aceitáveis de desempenho, além de manter os seus equipamentos de informática com softwares e aplicativos especializados, para facilitar a comunicação e otimizar o fluxo da informação e do conhecimento, permitindo, assim, o aumento da eficiência e das condições de excelência das informações armazenadas no sistema utilizado pelas bibliotecas, seja no campo da pesquisa, do ensino, da extensão, da prestação de serviços ou da gestão institucional.

A fim de destacar o cenário supracitado, concorda-se que:

> A chave para a compreensão dos problemas que existem na segurança dos computadores é o reconhecimento de que os problemas não são novos. São problemas antigos, desde o início da segurança informática (e, de fato, decorrentes de problemas paralelos no mundo não-computacional). Mas o *locus* mudou conforme o campo da computação mudou. Antes de meados dos anos 80, os computadores mainframe e de nível médio dominavam o mercado, e os problemas e soluções de segurança do computador eram expressos em termos de segurança de arquivos ou processos em um único sistema. Com a ascensão da rede e da Internet, a arena mudou. Estações de trabalho e servidores, e a infraestrutura de rede que os conecta, agora dominam o mercado. No entanto, se as estações de trabalho e os servidores, e a infraestrutura de rede de suporte são vistos como um sistema único, os modelos, teorias e declarações de problemas desenvolvidos para sistemas antes de meados dos anos 1980 se aplicam igualmente a sistemas atuais. (BISHOP, c2003, Prefácio, p. XXXIII, tradução nossa).

Nesse contexto, pretende-se levar adiante uma discussão acerca da segurança da informação nos ambientes das BUs, visando a inserção do bibliotecário como mais um profissional atuante nas principais tomadas de decisão no que se refere a propor sugestões, melhorias, soluções de problemas e/ou diretrizes que norteiem o acesso aos computadores das BUs, bem como na criação de uma política de segurança da informação voltada para esses ambientes. Aliado a isso, o bibliotecário possui, ainda, outro desafio relacionado à questão da segurança da informação, que é o de prover e garantir acesso livre à Internet. No entanto, de que maneira chegar a um consenso, ou a um meio-termo, em uma questão que causa polêmica e divide opiniões entre os próprios profissionais da área? Com relação a essa questão, e com base em constatações feitas no ambiente de trabalho que possibilitou este estudo, os profissionais da área de Tecnologia da Informação (TI) lidam bem melhor com o problema, tendo em vista que o tema faz parte de seu *metiê*, e, dentro disso, há propostas de imposição de medidas de controle de acesso para a melhor adequação do uso dos recursos disponíveis e dos computadores.

Trazendo essa discussão para a área biblioteconômica, a *International Federation of Library Associations and Institutions* (IFLA) e a *United Nation Educational, Scientific and*

Cultural Organization (UNESCO) elaboraram, em 2006, as Diretrizes para o Manifesto sobre a Internet, um documento que tem como ponto de partida o Manifesto da IFLA sobre a Internet, publicado em 2002, o qual já vem dando ampla e útil orientação desde então. Contudo, é preciso considerar o fato de que, desde aquela época, o cenário da Internet, dos usuários e da segurança da informação tem mudado consideravelmente. Aliás, até mesmo as Diretrizes que foram elaboradas em 2006, que vêm sendo traduzidas para outros idiomas e endossadas pela IFLA, apresentam algumas recomendações que permanecem as mesmas desde aquele período. Portanto, o tema mostra-se extremamente oportuno para discussão num período de mudanças na Internet e de seus usuários, assim como os diversos marcos regulatórios que vêm surgindo e gerando novos embates.

Como exemplo, tem-se a Lei 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet (MCI). Essa lei, de iniciativa do Poder Executivo Federal, tem por objetivo estabelecer os "[...] princípios, garantias, direitos e deveres para o uso da Internet no Brasil." (BRASIL, 2014). O Marco Civil da Internet tem o desafio de contribuir para a construção de "[...] uma internet que seja viável, acessível e justa para todos." (NAZARENO, 2014, p. 27), e justamente por isso pretende estabelecer os direitos e as responsabilidades que todos os sujeitos (usuários, provedores de conteúdo, provedores de conexão, detentores de direitos autorais e governo) relacionados à Internet no país possuem. O MCI deixa clara a necessidade de serem estabelecidos parâmetros para o acesso seguro do conteúdo disponível na Web, e esses parâmetros não devem apenas existir no plano nacional, mas também no âmbito institucional local, por meio da realização de ações que estimulem a segurança da informação.

O Comitê Gestor da Internet no Brasil (CGI.br) ([2016]) mantém dentro de seu website uma seção exclusiva para as discussões sobre o MCI, a qual enfatiza que a segurança, estabilidade e resiliência da Internet devem ser objetivos fundamentais de todas as partes interessadas na governança da Internet; portanto, a Internet deve ser um ambiente estável, resistente, seguro e confiável. Além disso, esclarece que a eficácia na abordagem dos riscos e ameaças à segurança e estabilidade da Internet depende de uma forte cooperação entre os diferentes intervenientes.

Nesse sentido, o desenvolvimento deste estudo se fez necessário objetivando não apenas traçar diretrizes para uso e manutenção dos computadores e para acesso à rede Wi-Fi das bibliotecas onde uma pesquisa-ação foi realizada, mas também com a finalidade de contribuir com a proposta de implantação de uma Política de Segurança da Informação (PSI) para o Sistema de Bibliotecas da Universidade Federal do Ceará (UFC), atendendo, assim, às Normas Internacionais de Segurança da Informação em Bibliotecas (ISO 27001 e ISO 17799), além de contemplar um dos objetivos previstos no Plano de Desenvolvimento Institucional (PDI) da referida instituição (UNIVERSIDADE FEDERAL DO CEARÁ, 2012). É importante ressaltar que a segurança da informação vai muito além da simples manutenção e do diagnóstico de problemas em computadores, embora isso seja um dos aspectos que envolvem a área e a

consequente discussão sobre o assunto, afinal, grande parte das informações geradas nesses ambientes advém dos computadores, conforme será visto a seguir.

2 PRINCIPAIS CONCEITOS E A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NAS INSTITUIÇÕES

Visando a proposta de inserção do bibliotecário como profissional atuante no planejamento, na elaboração e/ou na implantação de políticas institucionais centradas na segurança da informação, fez-se necessário recorrer à teoria, a alguns dos documentos normativos existentes e à legislação vigente acerca da importância da segurança da informação nas instituições, e também sobre as principais pragas virtuais às quais todos os computadores estão suscetíveis. Aliado a isso, serão abordados os princípios e a definição de PSI.

No contexto da segurança da informação, a informação é um ativo essencial do ponto de vista de negócio de uma organização e, consequentemente, deve ser devidamente protegida (ABNT NBR ISO/IEC 27002, 2013). Nesse sentido, Mandarino Júnior (2010) conceitua informação como um bem incorpóreo, intangível e volátil, e seus ativos tornam-se os principais focos de atenção quanto à segurança da informação. São exemplos de ativos de informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários; os sistemas utilizados; os locais onde se encontram esses meios e os recursos humanos que a eles têm acesso (MANDARINO JÚNIOR, 2010).

A informação pode ser considerada o bem de maior valor para empresas privadas e para órgãos públicos, assim como o recurso patrimonial mais crítico, pois quando adulterada, indisponível ou acessada por pessoas de má-fé sem a devida autorização, ou por concorrentes, a imagem da instituição pode ser significativamente comprometida, assim como o andamento dos próprios processos institucionais, ou seja, a continuidade de uma organização pode ser comprometida se não for dada a devida atenção à segurança de suas informações (BRASIL, [2014]). Considera-se, então, que:

> Na sociedade da informação, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança da informação tornou-se um ponto crucial para a sobrevivência das instituições. (BRASIL, 2007, p. 2).

Por seu valor expressivo, a informação representa grande poder para quem a possui. Ademais, está integrada com os processos, pessoas e tecnologias. Para reforçar a importância da informação como um ativo de grande valia e recurso estratégico para as empresas privadas e instituições públicas, sob a visão da vantagem competitiva, a figura 1 ilustra bem essa realidade:

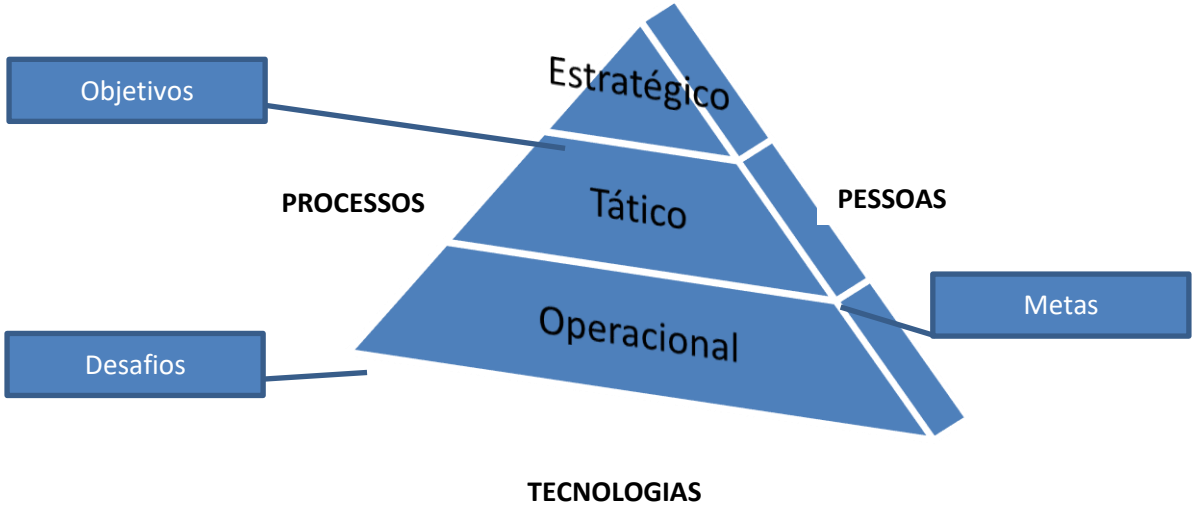

FIGURA 1. Papel estratégico da informação

Fonte: Elaborado pelos autores, baseado em Rezende e Abreu (2003).

A partir da compreensão desses níveis de gestão e de responsabilidades, e para que se possa levar essa discussão adiante, é preciso conceituar o termo "segurança da informação". De acordo com o Artigo 2º, inciso II, do Decreto nº 3.505, de 13 de junho de 2000, a segurança da informação é definida como:

> [...] proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. (BRASIL, 2000, online).

E é justamente nesse cenário que a segurança da informação se faz mais do que necessária nas instituições, tendo em vista não apenas a garantia do acesso seguro e da disponibilidade das informações, mas também o cumprimento da legislação estabelecida pelo Gabinete de Segurança Institucional da Presidência da República (GSIPR), por intermédio do Departamento de Segurança da Informação e Comunicações (DSIC). Há também o Comitê Gestor de Segurança da Informação (CGSI), que auxilia o referido GSIPR. O CGSI é composto por representantes de órgãos da Administração Pública Federal (BRASIL, 2016): Ministério da Justiça e Cidadania; Ministério da Defesa; Ministério das Relações Exteriores; Ministério da Fazenda; Ministério do Trabalho; Ministério da Saúde; Ministério da Indústria, Comércio Exterior e Serviços; Ministério do Planejamento, Desenvolvimento e Gestão; Ministério da Ciência, Tecnologia, Inovações e Comunicações; Casa Civil da Presidência da República; Ministério de Minas e Energia; Ministério da Transparência, Fiscalização e Controladoria-Geral da União; Advocacia-Geral da União; e Secretaria de Governo da Presidência da

República, sendo que os trabalhos são coordenados pelo GSIPR, na condição de Secretaria-Executiva do Conselho de Defesa Nacional (CDN).

A existência de cada um desses órgãos norteia e valida as ações com vistas à segurança da informação nas instituições, dentre elas as BUs. Contudo, de nada adianta pensar numa PSI que contemple o ambiente das BUs se não se conhecer, ainda que superficialmente, os principais conceitos de segurança da informação e sua importância, por que se deve preocupar-se, quais são os tipos de pragas virtuais e ameaças internas e externas a que as BUs estão suscetíveis.

2.1 Princípios e Política de Segurança da Informação

Um dos conceitos mais completos sobre segurança da informação é apresentado por Bishop (c2003, p. 15, grifo e tradução nossa):

> [...] **segurança** [da informação e] dos computadores não é apenas uma ciência, mas também uma arte. É uma arte porque nenhum sistema pode ser considerado seguro sem um exame de como ele deve ser usado. A definição de "computador seguro" **exige uma declaração de requisitos e uma expressão desses requisitos sob a forma de ações autorizadas e usuários autorizados**. (Um computador ocupado em uma universidade pode ser considerado "seguro" para os fins do trabalho realizado na universidade. Quando movido para uma instalação militar, esse mesmo sistema não pode fornecer controle suficiente para ser considerado "seguro" para fins do trabalho feito nessa instalação). Como as pessoas, assim como outros computadores, interagem com o sistema de computador? Quão clara e restritiva a interface criada por um designer em segurança pode tornar o sistema inutilizável ao tentar impedir o uso não autorizado ou impedir o acesso aos dados ou recursos no sistema? Assim como um artista pinta sua visão do mundo sobre a tela, o designer de recursos de segurança articula sua visão do mundo da interação homem/máquina na política de segurança e nos mecanismos do sistema. Dois designers podem usar desenhos inteiramente diferentes para conseguir a mesma criação, assim como dois artistas podem usar temas diferentes para alcançar o mesmo conceito.

Portanto, com base no exposto, pode-se considerar e resumir em linhas gerais que, para a criação de qualquer PSI, é obrigatória a apresentação de critérios e/ou diretrizes do que se pode ou não fazer nos computadores e por meio da rede utilizada, além de definir quem pode usar e de que forma deve utilizar esses equipamentos e recursos.

Conforme Concerino (2005, p. 155), a segurança da informação possui três pilares básicos. Apresentando-os em linhas gerais, são eles:

a) **Confidencialidade**: refere-se ao sigilo de informações. Busca assegurar que a informação será acessível somente às pessoas devidamente autorizadas. Quando alguma informação é vista ou copiada por alguém que não possui autorização para fazê-lo, este aspecto da segurança não está sendo observado;
b) **Integridade**: refere-se à impossibilidade de alteração de informações na rede. Visa salvaguardar os dados e as informações, garantindo, assim, a veracidade e autenticidade da

informação, bem como os seus métodos de processamento. A perda da integridade se dá quando, inexistindo a devida segurança, ocorre a modificação de um tópico importante, que pode ser alterado pelos mais surpreendentes motivos, até mesmo intencionalmente;
c) **Disponibilidade**: busca assegurar que dados, informações e sistemas estarão devidamente disponíveis sempre que solicitados. A ausência de disponibilidade ocorre quando a informação é deletada ou se torna inacessível ao usuário autorizado a consultá-la.

Na literatura da área, há mais princípios relacionados à segurança da informação, porém, para fins deste estudo, foram considerados apenas os três supracitados.

A classificação das informações nas organizações deve ser realizada a fim de assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância. Cada instituição deve rotular e tratar a informação de acordo com o seu próprio esquema de classificação (ABNT NBR ISO/IEC 27001, 2013).

A partir dessa classificação, têm-se os documentos sigilosos, compostos por dados ou informações cujo conhecimento irrestrito ou divulgação pode acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas. Esse tipo de informação e/ou documento deve receber medidas especiais de segurança (BRASIL, 2011). Por outro lado, a informação ostensiva é caracterizada por ser facilmente percebida e compreendida, dispensando qualquer esforço na sua assimilação. Nesse sentido, o Decreto nº 5.903, de 20 de setembro de 2006, dispõe e regulamenta, com base nas Leis nº 10.962 e nº 8.078, as práticas infracionais que afrontam o direito básico do consumidor de obter informação adequada e clara sobre produtos e serviços (BRASIL, 2006).

A cartilha de segurança da informação, elaborada pelo Superior Tribunal de Justiça (STJ), esclarece que:

> Um órgão que leva a Segurança da Informação a sério mantém os riscos e ameaças sob controle e não coloca em jogo a sua imagem organizacional. Com isso, toda a instituição ganha e mantém seu objetivo maior: prestar um serviço de qualidade para o cidadão brasileiro. (BRASIL, [2014], p. 16).

Complementando a recomendação da cartilha, à luz de Bishop (c2005), o autor esclarece que:

> [...] a Internet fornece apenas mecanismos de segurança mais rudimentares, que não são adequados para proteger as informações enviadas por essa rede. No entanto, atos como a gravação de senhas e outras informações confidenciais violam uma política de segurança implícita da maioria dos sites (especificamente, as senhas são propriedade confidencial de um usuário e não podem ser gravadas por ninguém). As políticas podem ser apresentadas matematicamente, como uma lista de não permitidos (não seguros). Para nossos propósitos, assumiremos que qualquer política

> fornece uma descrição axiomática de estados seguros e estados não seguros. (BISHOP, c2005, p. 7, tradução nossa).

Assim, é possível corroborar com João (2012, p. 58) quando afirma que:

> [...] segurança tem a ver com impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação. Já os controles garantem a segurança dos ativos da organização, a precisão e a confiabilidade de seus registros contábeis e a adesão operacional aos padrões administrativos.

Esse objetivo pode ser alcançado das seguintes maneiras: separar o ativo da ameaça física e/ou logicamente; destruir a ameaça ou mover/destruir o ativo. A destruição da ameaça torna-se inviável, pois, além de envolver um processo complexo, pode envolver ações ilegais. Destruir o ativo ameaçado é completamente indesejado do ponto de vista do dono do ativo, e movê-lo pode ser um processo muito custoso ou até mesmo impraticável. Portanto, resta separar, física/logicamente, o ativo da ameaça.

Para realizar essa separação, é necessário que o órgão, instituição ou organização adote uma PSI e implemente os mecanismos e procedimentos necessários para que esta política seja cumprida. Como definição de PSI, destaca-se:

> Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações. (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 10).

Para Bishop (c2005, p. 7, tradução nossa), é importante explicar a diferença entre PSI e os mecanismos de segurança:

> Definição 1-1. Uma política de segurança é uma declaração do que é e do que não é permitido. Definição 1-2. Um mecanismo de segurança é um método, uma ferramenta ou um procedimento para fazer se cumprir uma política de segurança. Mecanismos podem não ser técnicos, como exigir prova de identidade antes de alterar uma senha, na verdade, as políticas exigem frequentemente alguns mecanismos processuais que a tecnologia não pode impor.

Sobre os mecanismos de segurança da informação, destacam-se os controles físicos, os quais são considerados como barreiras que limitam o acesso direto à informação ou à infraestrutura, garantindo a existência da informação que a suporta. Para apoiar esses mecanismos de segurança (controles físicos: portas, blindagem, guarda etc.), há também os controles lógicos, que são barreiras que impedem ou limitam o acesso a informações que geralmente estão em ambiente controlado e eletrônico. Um dos mecanismos que apoia o controle lógico é a criptografia. Esta, por sua vez, permite codificar e transformar a informação de forma a torná-la ininteligível a terceiros, e, para tal, determinados algoritmos e chaves

secretas são utilizadas para produzir uma sequência de dados criptografados a partir de dados não criptografados. Como mecanismos lógicos, pode-se citar também: a assinatura digital; as funções de "*Hashing*" ou de checagem; os mecanismos de controle de acesso (senhas, palavras-chave, biometria, *firewalls*, entre outros); e os mecanismos de certificação e de integridade e o *Honeypot*, programa cuja função é detectar e impedir a ação de um *cracker*, *hacker* e *spammer*, ou de qualquer outro agente externo. Existem, ainda, diversas ferramentas e sistemas voltados para a segurança, como os antivírus, *firewalls*, filtros AntiSpam, dentre outros.

A cartilha de segurança para Internet do Comitê Gestor da Internet no Brasil (CGI.br) (2012, p. 47-48) considera como requisitos básicos de segurança:

- **Identificação**: permitir que uma entidade se identifique, ou seja, diga quem ela é;
- **Autenticação**: verificar se a entidade é realmente quem ela diz ser;
- **Autorização**: determinar as ações que a entidade pode executar;
- **Integridade**: proteger a informação contra alteração não autorizada;
- **Confidencialidade ou sigilo**: proteger uma informação contra acesso não autorizado;
- **Não repúdio**: evitar que uma entidade possa negar que foi ela quem executou uma ação;
- **Disponibilidade**: garantir que um recurso esteja disponível sempre que necessário.

A segurança da informação não é somente TI, pois envolve legislação, normas técnicas, negócio e tecnologia, e todos esses fatores devem ser levados em consideração na elaboração de uma PSI. Diante disso, Vieira (2014) elaborou uma compilação da legislação específica relacionada à segurança da informação (atualizada até 14 de agosto de 2014), na qual contempla: Dispositivos Legais de Caráter Federal; Legislação Específica de Caráter Federal; Legislação Específica de Caráter Estadual/Distrital; Legislação Específica de Caráter Municipal; Normas Técnicas; Projetos de Leis (VIEIRA, 2014).

A gestão da segurança da informação e a sua implantação nas organizações devem ser realizadas também em conformidade com as normas da ABNT, mais especificamente da "família 27000", e entre outras relacionadas. Além disso, é importante se ter uma noção acerca do tema e dos assuntos relacionados, tais como: erros inerentes à utilização e manipulação de dados (exemplo: um e-mail encaminhado para o destinatário errado); ataques à rede, roubo de dados, falsificações etc.; ações da natureza (terremotos, tempestades, inundações, dentre outras intempéries) que possam comprometer as estruturas físicas, inclusive as que salvaguardam dados de *backup*; prejuízos financeiros, processos judiciais, multas ou penalidades contratuais; danos à imagem; e sobre as principais pragas e ameaças virtuais que deixam os recursos informáticos vulneráveis a ataques, roubo e manipulação de dados.

2.2 Pragas Virtuais

Conforme o apresentado na seção anterior, a segurança da informação também é uma ciência. Sua teoria é baseada em construções matemáticas, análises e provas. Seus sistemas são

construídos de acordo com as práticas aceitas de engenharia. Usa raciocínio indutivo e dedutivo para examinar a segurança dos sistemas de axiomas-chave e descobrir princípios subjacentes. Esses princípios científicos podem, então, serem aplicados a situações não tradicionais e a novas teorias, políticas e mecanismos (BISHOP, c2003, p. 15). Dentro desse universo, uma das ocorrências mais comuns é a proliferação de pragas virtuais que podem comprometer inexoravelmente a segurança das informações e dos computadores.

Em nível deste estudo, os vírus, *malwares* e *worms* serão considerados como sendo as principais pragas ou ameaças virtuais a que os computadores estão constantemente suscetíveis. Conforme João (2012), o termo genérico para programas de software mal-intencionado é conhecido como *malware*. Relacionando vírus e *malwares*, João (2012, p. 60) descreve que

> [...] eles podem ser de vários tipos, incluindo vírus de computador, *worms* e cavalos de Tróia. Um vírus de computador é um programa que se anexa a outros para ser executado normalmente, sem que o usuário perceba. A maioria dos vírus de computador transporta uma carga, que pode não causar grandes danos (apenas mostrando uma mensagem ou imagem, por exemplo), ou ser altamente destrutiva, arruinando programas, dados e até mesmo reformatando o disco rígido, entre outras coisas [...]

Certamente, tomando como base a práxis profissional ou o uso pessoal dos computadores, são muitos os alertas sobre o fato do quanto é perigoso fazer download de arquivos de fontes desconhecidas e/ou duvidosas, e isso se deve ao fato de os vírus serem comumente transmitidos de um computador para o outro, seja por envio de um e-mail com anexo ou cópia de um arquivo infectado, seja por outras diferentes ações.

Conceituando *worms* (vermes, em inglês), João (2012, p. 62) afirma que

> [...] consistem em programas de computador independentes, que se copiam de um computador para o outro por meio de uma rede. E a diferença dos vírus para os *worms* é que estes [...] podem funcionar sozinhos, sem se anexar a outros arquivos, e também não dependem do comportamento humano para se espalhar [...]

Por essa razão, os *worms* são disseminados bem mais rapidamente do que os vírus e agem destruindo programas, arquivos, dados etc., interferindo até no funcionamento das redes de computadores. Costuma-se afirmar que uma das características que demonstram que um computador possui *worms* é exatamente a lentidão e o travamento da máquina, pois uma de suas ações é justamente interromper e prejudicar o funcionamento dos computadores.

Para prevenir esses e outros tipos de problemas relacionados à rede, Herzog (2010) esclarece que a segurança consiste em separar o ativo das ameaças, ou seja, "a segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela organização." (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 9).

Diante de todo esse aporte teórico, também documentado em forma de Decretos, Leis e de documentos institucionais, será apresentada, a seguir, a discussão acerca da atuação do bibliotecário como um dos profissionais atuantes (trabalhando em conjunto com os profissionais de TI) no planejamento, na elaboração e na implantação de uma PSI voltada para os ambientes das BUs.

2.3 Atuação do Bibliotecário diante da Segurança da Informação

Acerca das competências e da atuação profissional do bibliotecário no contexto da segurança da informação, Sobral (2012, online, grifo nosso) esclarece que:

> De acordo com a Classificação Brasileira de Ocupações – CBO – o Bibliotecário pertence à família dos profissionais da informação. Suas principais atribuições são: disponibilizar a informação em qualquer suporte; gerenciar unidades como bibliotecas, centros de informação e correlatos, além de redes e sistemas de informação; tratar tecnicamente e desenvolver recursos informacionais; disseminar informação com objetivo de facilitar o acesso e geração do conhecimento; desenvolver estudos e pesquisas; realizar difusão cultural e desenvolver ações educativas. Para cumprir um trabalho de tamanha responsabilidade, é necessário, antes de tudo, **garantir a segurança da informação gerenciada**, que **não se trata apenas do conceito usual que temos de segurança**, que é garantir apenas que algo não seja perdido ou que caia nas mãos erradas. **A segurança da informação é também garantir que a informação esteja disponível quando necessária, e que se possa garantir a sua integridade**.

Nesse sentido, independente da natureza e do público a que uma determinada biblioteca se destine, se a sua gestão não se sensibilizar com a questão da segurança da informação, a biblioteca estará sujeita a graves problemas, como, por exemplo, a má utilização dos computadores destinados à pesquisa, inclusive gerando riscos de roubo, vazamento e/ou perda de dados. No entanto, também é preciso levar em consideração a conduta dos usuários, pois muitos deles não tomam o devido cuidado ao utilizar computadores de acesso público, especialmente quando acessam e-mails e os esquecem abertos, ou ao acessarem o sistema online de empréstimo para verificar suas posições na fila de espera da reserva, também esquecem de encerrar a sessão, dentre muitos outros exemplos que poderiam ser citados. Afinal, implicitamente, os usuários esperam e confiam que a biblioteca é a responsável por manter seguros os seus dados e os equipamentos disponíveis em bom estado, embora não tenham tido qualquer informação ou sensibilização para a causa, demonstrando que o bibliotecário está diante de mais um desafio: educar esses usuários e prepará-los para novas práticas e condutas simples com relação à segurança de seus dados e dos outros. Diante dessas ameaças e situações, nota-se o quanto as bibliotecas devem estar preparadas para lidar com esses problemas.

Cabe aqui introduzir uma discussão relevante, na qual não haverá aprofundamento por não ser o objetivo principal deste artigo: quais são as possibilidades de utilização dos computadores de uma biblioteca? Para pesquisa? Para elaboração de trabalhos acadêmicos? Para acessar diversos conteúdos na Internet? Para acessar as redes sociais? Todas essas

perguntas, e muitas outras que não foram feitas, são importantes para saber a que perigos a rede da biblioteca está exposta e, assim, poder traçar (em parceria com a equipe de segurança da informação e/ou informática da instituição) qual será a melhor estratégia operacional de enfrentamento dos riscos para lidar com essas circunstâncias, sem limitar as possibilidades, liberdades e direitos dos usuários, e, ao mesmo tempo, preservar e resguardar seus dados. Além disso, um bom plano de ação também se faz necessário, visando à proteção da rede contra ataques e vulnerabilidades, e ainda salvaguardar e preservar os computadores e equipamentos da biblioteca, afinal, como se verá adiante, diversos computadores das bibliotecas podem estar desprotegidos, tornando-se alvos de ataques, espionagens e instalação de softwares piratas que geram a proliferação de vírus e *malwares*, sequestro de dados, acesso indevido a toda a rede, dentre outros males.

Concernente à segurança da informação, os gestores das instituições precisam estar cientes de que não basta apenas traçar um esboço de uma política, pois, é preciso que esse documento contenha diretrizes consistentes. Esse fato reforça ainda mais a visão de que as BUs têm a necessidade de que se estabeleça o quanto antes sua política, tendo em vista que existem leis, decretos e determinações federais que validam a existência de uma PSI nas instituições. Como exemplo, tem-se o Decreto nº 3505, de 13 de junho de 2000 (BRASIL, 2000), que institui a PSI nos órgãos e nas entidades da Administração Pública Federal. Obviamente, a implementação e aplicação de uma PSI devem ser estabelecidas para a instituição como um todo, independente de que seja na esfera pública ou privada, incluindo as bibliotecas. Contudo, essa política deve ser pensada, planejada e elaborada em parceria com o setor responsável pelo suporte em TI, além de ser bem estruturada, para atender ao objetivo a que ela se propõe. Acerca da consistência de uma PSI, concorda-se que:

> As políticas de segurança devem ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção. Deve também adaptar-se a alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques. (WEB ANEXO TECHNOLOGY, 2011, online).

Além disso, defende-se a ideia de que, assim como o bibliotecário deve exercer o seu papel no planejamento da elaboração desse documento, é preciso que haja uma divisão de responsabilidades dentre os setores da instituição, contemplando a biblioteca nas diretrizes e nas ações estabelecidas em comum acordo. Nesse sentido,

> É recomendável que na estrutura da organização exista uma área responsável pela segurança de informações, a qual deve iniciar o processo de elaboração da política de segurança de informações, bem como coordenar sua implantação, aprová-la e revisá-la, além de designar funções de segurança. Vale salientar, entretanto, que pessoas de áreas críticas da organização devem participar do processo de elaboração da PSI, como a alta administração e os diversos gerentes e proprietários dos sistemas informatizados. Além disso, é recomendável que a PSI seja aprovada pelo mais alto

> dirigente da organização. (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 10).

No âmbito das BUs, o planejamento de uma PSI envolve algumas restrições de acesso. Esse fato pode gerar alguma estranheza no usuário, porém, acredita-se que o bibliotecário pode e deve adotar uma atitude que vise sensibilizar o usuário acerca da importância da segurança da informação. Adotando essa postura, é preciso estar preparado para se deparar com situações de insatisfação por parte de alguns dos usuários e com o embate de ideias que causem uma discussão saudável dentre a classe bibliotecária e os usuários, no que concerne às medidas propostas na PSI, além de se ter em mãos mais um indicador a ser avaliado nas bibliotecas, com a finalidade de atingir a rapidez, precisão e segurança nos serviços oferecidos por meio do uso dos computadores.

Com relação às restrições de acesso, estas devem ser contempladas na PSI, e é necessário salientar que:

> **O fato de um usuário ter sido identificado e autenticado não quer dizer que ele poderá acessar qualquer informação ou aplicativo sem qualquer restrição**. Deve-se implementar um controle específico, restringindo o acesso dos usuários apenas às aplicações, arquivos e utilitários imprescindíveis para desempenhar suas funções na organização. Esse controle pode ser feito por menus, funções ou arquivos. (BRASIL, 2007, p. 18, grifo nosso).

Como se pode notar, estabelecer uma PSI também está diretamente ligado a ações que podem ser consideradas contraditórias ou polêmicas para os usuários; porém, todas essas más impressões se desfazem com a educação constante dos usuários, com a ampla divulgação da PSI dentro da instituição e com a consolidação de uma PSI pautada nos princípios da segurança da informação, sendo preferencialmente gerida por uma instância maior do que a das BUs, sempre apoiada pela equipe de TI e pela autoridade máxima do órgão. No entanto, quaisquer que sejam as tomadas de decisão, elas precisam estar documentadas e padronizadas com o objetivo de que todos (sem exceção) cumpram as diretrizes estabelecidas na PSI. Partindo desse princípio, Guelman (2006, p. 1) corrobora que "De nada adianta investir em tecnologia e proteção física se não temos a colaboração e o comprometimento das pessoas."

O bibliotecário deve enfrentar, ainda, outro desafio relacionado à questão da segurança da informação, que é o de prover e garantir acesso à Internet, conforme o trecho que se segue, retirado das Diretrizes para o Manifesto sobre a Internet (2006) da IFLA/UNESCO:

> [A declaração enfatiza] uma sociedade centrada nas pessoas, inclusiva e orientada ao desenvolvimento, onde todos possam acessar e compartilhar conhecimentos em uma atmosfera de acesso irrestrito à informação e à liberdade de expressão [...] [Esboça] políticas e procedimentos de serviços que salvaguardam a liberdade de acesso à informação para todos os usuários de bibliotecas e asseguram que o acesso à Internet é livre, equitativo e livre de restrições desnecessárias. (INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS; UNITED NATION EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION, 2006, p. 10).

Contudo, é importante ressaltar que o próprio documento tem como ponto de partida o Manifesto da IFLA sobre a Internet que já vem dando ampla e útil orientação desde 2002, e, nos últimos anos, o cenário da Internet, dos usuários e da segurança da informação tem mudado consideravelmente. Outro documento de destaque são as Diretrizes elaboradas em 2006, que, desde então, vêm sendo traduzidas para outros idiomas e endossadas pela IFLA, ou seja, algumas recomendações permanecem as mesmas desde aquela época. O mesmo conjunto de Diretrizes alerta para o fato de que:

> **A tecnologia muda; as concepções do que são assuntos importantes mudam; e nenhum conjunto de diretrizes pode ser visto como válido por muito tempo.** Se esse documento diz menos do que se poderia esperar sobre um assunto que ocupava lugar importante na preocupação de todo o mundo há cinco anos atrás, é porque isso, provavelmente, tem que ser assim. Se não há uma clara orientação (como deveria ser desejável) sobre algo que pode vir a ser o centro das preocupações daqui a doze meses, é porque os redatores não possuem o poder da clarividência. (INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS; UNITED NATION EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION, 2006, p. 4, grifo nosso).

As Diretrizes da IFLA/UNESCO (2006, p. 15) também afirmam: "Ainda que a filtragem seja um dos assuntos com maior probabilidade de causar polêmicas nas bibliotecas, outras desvantagens da Internet têm que ser consideradas." As referidas Diretrizes reconhecem ainda que é possível criar uma Política de Uso Aceitável, do inglês *Acceptable Use Policy* (AUP), a qual:

> [...] torna os usuários da Internet na biblioteca conscientes do que é o uso aceitável ou não aceitável dos computadores da biblioteca, e de quais sanções existem se os bibliotecários violarem a política. Mesmo sendo provável que as AUPs difiram de uma biblioteca para outra, é provável que algumas partes sejam comuns a todos - por exemplo, aquelas que tratam do uso ilegal de equipamentos (por exemplo, usando o computador da biblioteca para acessar outros computadores sem permissão). **Uma AUP deve informar os usuários sobre suas responsabilidades, o que inclui tanto exigências legais com aquelas definidas pela biblioteca. A política deve fornecer à biblioteca proteção legal por responsabilidade, tornando claro para os usuários que a biblioteca não é responsável por suas ações em linha relativas ao e-comércio e possível fraude por terceiros que resultem em prejuízos para eles.** Por exemplo, uma AUP tornaria claro que todas as transações em linha são por conta e risco do usuário e não são responsabilidades da biblioteca. **O propósito geral de uma AUP é estabelecer um contrato entre a biblioteca e o usuário - a política deve definir os limites do serviço, estabelecendo que serviços estão disponíveis e o que a levou a não disponibilizar certos serviços**. (INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS; UNITED NATION EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION, 2006, p. 42, grifo nosso).

Portanto, as BUs precisam e devem elaborar documentos que visem ao estabelecimento de normas gerais de utilização dos equipamentos e recursos computacionais destinados à pesquisa, ao ensino, à extensão e às atividades administrativas das Instituições de Ensino Superior, a fim de que as ameaças sejam evitadas e/ou amenizadas. Ao criar políticas

institucionais, tais como diretrizes, normas e regras, estas devem complementar a PSI da instituição, e não substituir as políticas existentes, nem mesmo outros documentos que se apliquem à utilização dos equipamentos e dos recursos informáticos.

3 MATERIAIS E MÉTODOS

O estudo realizado utiliza-se da pesquisa-ação como metodologia norteadora para a realização dos trabalhos. De acordo com Elliot (1997, p. 17), a pesquisa-ação é um processo que se modifica continuamente em espirais de reflexão e ação, onde cada espiral inclui:

• Aclarar e diagnosticar uma situação prática ou um problema prático que se quer melhorar ou resolver;
• Formular estratégias de ação;
• Desenvolver essas estratégias e avaliar sua eficiência;
• Ampliar a compreensão da nova situação;
• Proceder aos mesmos passos para a nova situação prática.

A figura 2 explicita sucintamente esse ciclo:

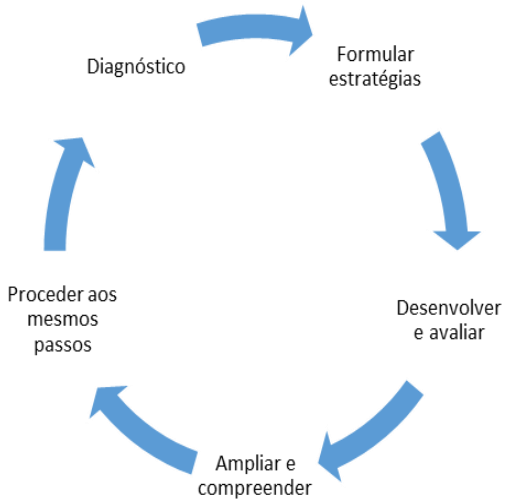

FIGURA 2. Espirais da pesquisa-ação.

Fonte: Elaborado pelos autores, baseado em Elliot (1997, p. 17).

Inicialmente, uma comissão composta por seis bibliotecários se reuniu para delinear os passos e as ações a serem seguidas para a realização de visitas *in loco*, realizadas em todo o Sistema de Bibliotecas da UFC, sendo 19 bibliotecas no total. Assim, foi estabelecida uma parceria entre a comissão formada, a direção do Sistema de Bibliotecas e a Secretaria de

Tecnologia da Informação (STI) da Universidade, o que resultou na elaboração de um cronograma de visitas às bibliotecas da capital e uma do interior (somando-se 14 bibliotecas).

Além das visitas realizadas em cada biblioteca, observações e intervenções feitas no serviço de referência de cada unidade foram consideradas e registradas em formulário durante a visitação, tendo em vista que é o local onde se recebem os usuários, auxiliando-os em suas pesquisas, e, inclusive, é o espaço onde foram registrados os problemas percebidos com relação à utilização dos computadores. Com relação ao formulário como instrumento de coleta de dados, destinado para o registro da situação e diagnóstico dos computadores de pesquisa nas bibliotecas, Vergara (2000, p. 55) o considera como sendo "um meio-termo entre entrevista e questionário." Para Appolinário (2004, p. 100), o formulário é "Instrumento de pesquisa, similar a um questionário, porém, a ser preenchido pelo próprio pesquisador (e não pelo sujeito de pesquisa)." O pré-teste do formulário elaborado foi realizado nas bibliotecas que atendem às áreas de Ciências Humanas, Linguística, Letras e Artes, aliás, estas eram as unidades onde se apresentaram os casos mais graves encontrados.

Outra característica desta pesquisa é a sua natureza aplicada, descritiva e de cunho qualitativo. De acordo com Barros e Lehfeld (2000, p. 78), a pesquisa aplicada tem como motivação a necessidade de produzir conhecimento para aplicação de seus resultados, com o objetivo de "contribuir para fins práticos, visando à solução mais ou menos imediata do problema encontrado na realidade". Complementando essa afirmação, Appolinário (2004, p. 152) salienta que pesquisas aplicadas têm o objetivo de "resolver problemas ou necessidades concretas e imediatas".

Para complementar os procedimentos metodológicos, recorreu-se à pesquisa bibliográfica, com a finalidade de compor o referencial teórico. Além disso, com o preenchimento do formulário, surgiu a demanda de uma análise documental e de conteúdo após as visitas, pois ficou constatado que são técnicas que se complementam em relação ao objeto de estudo proposto.

Após o período de visitas, com base nos dados obtidos, a comissão de bibliotecários traçou como meta a elaboração de relatórios, com a finalidade de documentar a realidade encontrada nas bibliotecas. A partir desses relatórios, foram sugeridas medidas a serem adotadas em cada unidade, visando à solução dos problemas encontrados a fim de nortear futuras tomadas de decisão.

Nesse sentido, foi imprescindível recorrer à análise de conteúdo, que pode ser conceituada como sendo um conjunto de operações intelectuais que tem por objetivo descrever e representar o conteúdo dos documentos de uma forma distinta da original, visando a garantia da recuperação da informação nele contida e possibilitar seu intercâmbio, difusão e uso (IGLESIAS; GÓMEZ, 2004). Portanto, tal técnica é considerada como o tratamento do conteúdo, de forma a apresentá-lo de maneira diferente da proveniente fonte examinada, facilitando sua consulta e referenciação, ou seja, tem por objetivo dar forma conveniente e

representar de outro modo essa informação, por intermédio de procedimentos de transformação (BARDIN, 1997).

Passou-se, então, à análise do conteúdo dos relatórios elaborados com base na coleta de dados realizada em cada visita às bibliotecas. O conteúdo desses relatórios apresenta dados referentes aos campos do formulário, tais como: número de patrimônio do computador, sistema operacional da máquina, antivírus utilizado, editores de texto instalados, *player* de vídeos e músicas, histórico de acesso nos *browsers*, programas instalados, responsável pela manutenção dos computadores na unidade de informação, frequência de solicitação de manutenção, acesso à Internet Wi-Fi e informações complementares.

Por fim, ressalta-se que as diretrizes para uso e manutenção dos computadores destinados aos usuários do Sistema de Bibliotecas da UFC, assim como as diretrizes para o acesso à Internet sem fio (rede Wi-Fi) nas dependências das bibliotecas, foram construídas como resultado do trabalho, tendo em vista a necessidade de padronização no que se refere à configuração dos computadores disponibilizados para a comunidade acadêmica. Aliado a isso, houve a necessidade de a direção contribuir para a difusão da segurança da informação no Sistema de Bibliotecas, indo diretamente ao encontro da proposta da Política de Segurança da Informação e Comunicação (POSIC) elaborada pela própria STI da instituição (UNIVERSIDADE FEDERAL DO CEARÁ, 2013). Todas as diretrizes e documentos foram traçados após as etapas supracitadas e possibilitaram o desenvolvimento deste estudo, cujos resultados serão apresentados a seguir, mais especificamente o diagnóstico e os problemas evidenciados nas visitas às bibliotecas e, com base nas diretrizes elaboradas, os principais tópicos que devem constar na estrutura de uma PSI.

4 RESULTADOS

Os resultados desta pesquisa serão descritos com base nos problemas encontrados durante as visitas nas bibliotecas, cujo relatório possibilitou a elaboração de diretrizes norteadoras quanto ao uso e à manutenção dos computadores destinados aos usuários, bem como a sugestão de padronização do acesso à rede Wi-Fi nas dependências das bibliotecas. Além disso, a descrição da estrutura de uma PSI também será abordada como parte dos resultados alcançados.

4.1 Diagnóstico e Problemas Evidenciados a partir das Visitas às Bibliotecas

As bibliotecas visitadas estão inseridas em uma comunidade diversa de usuários, que variam de acordo com as grandes áreas do conhecimento e com os cursos de graduação e de pós-graduação da Universidade. Contudo, mesmo dentro dessa diversidade, alguns pontos em comum foram identificados. Dessa forma, os problemas evidenciados serão apresentados com base nesses pontos em comum, com o objetivo de evitar repetições desnecessárias e resguardar os nomes das bibliotecas em questão.

Primeiramente, foi contabilizada a quantidade de computadores disponíveis para os usuários em cada biblioteca, e se esses computadores eram destinados exclusivamente à consulta do acervo ou também para outras finalidades, como a produção de trabalhos acadêmicos e o acesso a mídias sociais, por exemplo. Constatou-se que, na maioria das bibliotecas, havia computadores específicos para ambos os casos: acesso exclusivo ao catálogo online, e aos demais serviços do Sistema de Bibliotecas, e acesso a sites fora do domínio da Universidade. Mesmo diante dessa realidade, foram encontrados problemas graves de infecção nas máquinas, o que tornou necessário um relato minucioso sobre cada situação.

Outra questão documentada foi acerca da manutenção dos computadores, mais especificamente quem a realiza (se profissional da biblioteca ou da STI), com que frequência e com base em quais problemas detectados. Foi constatado que muitas das bibliotecas recorriam a um dos funcionários terceirizados que faziam parte da equipe, com o intuito de prestar suporte de menor grau de complexidade quanto aos problemas das máquinas, apesar de muitos desses funcionários não possuírem formação específica na área de informática, atuando, assim, em situações mais rotineiras. Em casos mais complexos, que requeriam conhecimentos mais avançados, a maioria das bibliotecas acionava os serviços especializados da STI.

Na realidade encontrada nas bibliotecas, a maioria dos computadores utilizava sistema operacional Windows 7, programas instalados, editores de texto e visualizadores de vídeo, porém, alguns com áudio desabilitado, apesar dos visualizadores de vídeo estarem ativados. Em muitos dos computadores, as atualizações do Windows estavam pendentes. Um aspecto preocupante evidenciado foi o fato de muitas máquinas não possuírem nenhum programa antivírus instalado ou atualizado. Isso demonstra, claramente, como os computadores estavam completamente vulneráveis a ataques de vírus, *malwares* e *hackers*. Essa situação também ilustra um excesso de confiança por parte dos universitários, que acreditam estar protegidos ao utilizar os computadores da biblioteca ou navegar apenas por domínios seguros, mas, na verdade, nem sempre estão cientes dos riscos existentes no uso da Internet.

Outro aspecto crítico foi o fato de nem todos os computadores possuírem software dedicado ao controle de permissão de acesso a sites e à execução de aplicativos. Essa ausência se refletiu em um histórico de acesso preocupante. Se, por um lado, havia acessos a buscadores Web, MSN Brasil, e-mails, Facebook, Biblioteca Digital de Teses e Dissertações (BDTD), Repositório Institucional (RI), catálogo online e a outros domínios de sites da Universidade; por outro lado também existiam significativos acessos a sites de download de programas desconhecidos e de origem duvidosa, além de visitas a domínios de sites infectados já relatados nas principais empresas de segurança na Internet e de antivírus. O acesso a sites não recomendados acabou por facilitar que ferramentas nocivas que interferem nas configurações se instalassem nos computadores.

Esse cenário evidencia que a adoção de medidas voltadas para a segurança dos computadores era incipiente até o momento da realização das visitas, o que acabou por originar

uma série de transtornos e situações potencialmente perigosas no que se referem à segurança da informação, tais como: computadores de trabalho serem vistos e a rede ser mapeada por um determinado usuário a partir de uma das máquinas de pesquisa, possibilidade de roubo de senha ou de acesso a contas pessoais dos usuários, *login* e dados de cartões de crédito e de compras online salvos nos computadores, dentre outras ocorrências encontradas.

Situações semelhantes foram evidenciadas em todas as bibliotecas. Essa frequência na ocorrência de determinados problemas indica tanto aspectos devem ser abordados prioritariamente no tocante à implementação de uma PSI, quanto a necessidade premente dos bibliotecários dedicarem maior atenção a tais questões, seja na elaboração de diretrizes e políticas institucionais, seja na educação e sensibilização dos usuários.

O quadro 1 apresenta, sucintamente, os problemas em comum que foram evidenciados nas visitas às bibliotecas:

QUADRO 1. Resultados dos problemas encontrados nas visitas às bibliotecas.[i]

ÁREAS DO CONHECIMENTO	Ciências Exatas e da Terra e Ciências Biológicas (07 bibliotecas); Ciências Sociais Aplicadas (04 bibliotecas); Ciências Humanas e Linguística, Letras e Artes (02 bibliotecas); Ciências da Saúde (01 biblioteca).
SISTEMA OPERACIONAL	Linux (Ubuntu e Kubuntu), Windows XP, Windows 7 e Windows 8.
ANTIVÍRUS	05 bibliotecas utilizam; 08 bibliotecas utilizam parcialmente (não está instalado em todas as máquinas ou a licença expirou); 01 biblioteca não utiliza.
PROBLEMAS ENCONTRADOS	Computadores com configurações obsoletas; atualizações do sistema operacional pendentes e diversas vulnerabilidades; infecções encontradas (vírus, vírus multiplataforma [ataca todos os tipos de sistema operacional], *malwares*, *spywares*, Cavalos-de-Troia, *backdoors*, *keyloggers*; grande quantidade de *hijackers*, *adwares*, *spams*; Programas Potencialmente Indesejáveis (PUP); aplicações enganosas e *worms*; computadores lotados de arquivos salvos pelos usuários; sinal de Internet Wi-Fi irrestrito, com divulgação de senha única para qualquer usuário e sem o devido controle na maioria das bibliotecas; a responsabilidade pela manutenção da rede Wi-Fi é compartilhada com outros setores em algumas bibliotecas pertencentes a esta categoria.
PRÁTICAS E CONTROLES ENCONTRADOS	Apenas 03 bibliotecas das 14 visitadas apresentavam software de controle de acesso e parental em seus computadores; contudo, as ferramentas demonstraram-se ineficazes diante dos problemas encontrados; Somente 02 bibliotecas utilizavam o acesso à rede W-Fi por acesso identificado pelo portal ou aplicativo WUFCNet.
SITES ACESSADOS	Bancos (Internet *Banking*); blogs diversos; catálogo online; Sistema de Bibliotecas da Universidade; e-mails; redes sociais diversas; sistema de informação acadêmica da Universidade; notícias e fofocas diversas; jornais diversos; compra coletiva; concursos; videoaulas; sites de compartilhamento de vídeos com extenso histórico de busca e acesso a novelas mexicanas; sites de compartilhamento de arquivos; jogos

	diversos; sites de operadoras de telefonia (serviço de envio de mensagens); bases de dados diversas; bibliotecas digitais; letras de músicas; sites de download de séries e filmes; lojas de compras online diversas; sites de revistas em quadrinhos japoneses (mangás); extenso histórico de busca sobre notícias de sexo; ferramentas de compartilhamento de slides diversos; dicionários online; Wikis.
PROGRAMAS INSTALADOS	Bancos (Internet *Banking*); editores de texto; extensões diversas para navegadores; gerenciadores de downloads; jogos diversos; leitores de PDF; *players* de áudio e vídeo; *plugins* de jogos 3D; programa de sincronização de anotações; programas de mensagens/chat; programas otimizadores de sistema operacional; softwares de gravação de CD/DVD; softwares de videochamadas; softwares de design e cálculos.
SOLICITAÇÃO DE MANUTENÇÃO	Sim (anualmente): 01 biblioteca; Sim (sem frequência estabelecida, depende da necessidade): 13 bibliotecas; Não: 0 (zero) bibliotecas.
QUEM EXECUTA	Funcionário da área de TI: 08 bibliotecas; Funcionário terceirizado: 05 bibliotecas; Bibliotecário: 04 bibliotecas; Funcionário técnico-administrativo sem vínculo com a STI: 03 bibliotecas; Funcionário técnico-administrativo da biblioteca: 02 bibliotecas. Observação: Nessa opção, algumas bibliotecas se encaixavam em mais de uma condição; portanto, em alguns casos, mais de um item foi assinalado no formulário.

Fonte: Elaborado pelos autores.

Conforme o panorama geral apresentado no quadro acima, traçado a partir da análise e diagnóstico dos computadores, é possível perceber a necessidade de alinhamento das ações e padronização do serviço ofertado pelas bibliotecas (computadores de pesquisa e de acesso livre). A partir dos resultados encontrados, foi elaborado um relatório para cada biblioteca, constando todo o diagnóstico, inclusive as sugestões de soluções a serem aplicadas, especialmente para as bibliotecas com os casos mais graves. Esses relatórios foram enviados para a direção do Sistema de Bibliotecas e, em seguida, encaminhados para cada um dos cargos de direção, com o respectivo relatório individual por biblioteca.

Ainda durante as visitas, foi levantada a questão do acesso à rede Wi-Fi em cada biblioteca. Das 14 bibliotecas visitadas, 12 mantinham acesso aberto de duas formas distintas: sem nenhuma restrição a usuários internos e externos ou por meio de senha própria, divulgando-a em cartazes e no balcão de atendimento. Em outras situações encontradas, uma das bibliotecas dispunha de rede sem fio, porém, a secretaria do curso era a responsável pelo controle do acesso e distribuição da senha apenas para usuários ligados ao curso atendido, ou seja, nem mesmo a biblioteca sabia ou possuía autonomia para isso. Somando-se a esse fato, uma outra biblioteca só tinha acesso à Internet via cabo, pois ainda não dispunha de infraestrutura necessária para oferecer o serviço de Internet sem fio, e também vivenciava situação semelhante à da biblioteca citada anteriormente (a secretaria do curso disponibilizava as senhas de acesso). Outro caso verificado nas visitas foi o fato de uma das bibliotecas não

possuir sinal Wi-Fi próprio, assim, compartilhava do acesso disponibilizado pelo Centro Acadêmico do curso atendido.

Contudo, duas bibliotecas da área de Ciências Exatas ofereciam o acesso Wi-Fi por meio do portal, e também aplicativo, denominado WUFCNet, desenvolvido pela Divisão de Redes de Computadores (DRC) da STI da Universidade, no qual o *login* do usuário é feito com o número de seu CPF e com a senha do Sistema Integrado de Gestão de Atividades Acadêmicas (SIGAA). Além dessas duas bibliotecas, havia outros setores da instituição que tinham acesso Wi-Fi por meio desse portal, embora ainda em fase de testes. Diante dessa realidade, a solução solicitada à STI foi a adequação de todas as bibliotecas para a devida utilização do aplicativo WUFCNet, por se apresentar uma forma de acesso mais seguro em termos de identificação do usuário, sendo, portanto, a escolhida, institucionalmente, como a forma padrão a constar nas diretrizes para o acesso à rede Wi-Fi nas dependências das bibliotecas, conforme se verá adiante.

4.2 Estrutura das Diretrizes e da Política de Segurança da Informação

Partindo dos problemas evidenciados, delinearam-se estratégias e diretrizes para o uso e a manutenção dos computadores e para o acesso à rede Wi-Fi nas dependências das bibliotecas (UNIVERSIDADE FEDERAL DO CEARÁ. BIBLIOTECA UNIVERSITÁRIA, 2015a, 2015b). No escopo do documento, foram especificados os objetivos, os procedimentos a serem adotados nas bibliotecas, a configuração dos computadores de pesquisa e de acesso livre e a responsabilidade pelo suporte técnico às máquinas.

Assim, os procedimentos definidos foram:

a) Acionar a STI sempre que houver a necessidade de instalação, manutenção e/ou reparo nos computadores destinados à pesquisa e ao acesso livre dos usuários, estendendo-se também às máquinas de trabalho das bibliotecas, uma vez que há uma equipe especializada unicamente em atender a essas demandas na Universidade;
b) Adequar o sistema operacional dos computadores (Windows ou Linux) à necessidade da biblioteca;
c) Reservar uma quantidade específica de computadores exclusivamente para pesquisa ao catálogo online, acesso aos recursos e serviços disponíveis no site da biblioteca e no domínio da Universidade;
d) Disponibilizar pelo menos um computador com softwares e/ou recursos específicos para possibilitar o acesso de pessoas com deficiência.

No que se refere à configuração dos computadores utilizados exclusivamente para pesquisa, as recomendações previstas nas diretrizes foram as seguintes:

a) Instalar o sistema operacional Linux nas máquinas de pesquisa, dependendo da configuração de fábrica do computador;
b) Manter instalados e atualizados o sistema operacional, os antivírus e os navegadores de Internet;
c) Criar conta e senha de administrador e de convidado em cada uma das máquinas (a senha de administrador ficando sob a responsabilidade de bibliotecários);
d) Bloquear a instalação de softwares piratas e/ou não autorizados, e também as páginas externas ao domínio da Universidade, com exceção daquelas caracterizadas como sendo de pesquisa acadêmica;
e) Instalar o DosVox (programa para deficientes visuais), leitores de tela NVDA (para Windows) ou Orca (para Linux), além de outros recursos de acessibilidade em ambos os sistemas operacionais;
f) Providenciar adesivos especiais para teclados, a fim de torná-los acessíveis para os usuários com baixa visão e/ou com outros problemas oculares parciais.

Para fins de composição das diretrizes, foram considerados computadores de acesso livre aqueles cujo acesso a domínios externos à Universidade (tais como: contas de e-mail, mídias sociais, buscadores Web, dentre outros) ou ao site da biblioteca está liberado. Diante disso, foi enfatizado, devido à exigência por parte da gestão de algumas das bibliotecas, que a disponibilização de computadores para esta finalidade não seria obrigatória, e mesmo aquelas que os possuam poderão suspender a oferta desse serviço a qualquer momento. Dessa forma, condicionou-se a configuração dessas máquinas às seguintes recomendações:

a) A quantidade de computadores reservados ao acesso livre dos usuários, bem como o seu tempo de permanência nos computadores, ficará a cargo da direção de cada biblioteca (houve casos em que foram realizados testes com softwares destinados a regular o tempo de permanência, ou que mesmo se designou um funcionário para este fim ou se configurou o próprio sistema operacional a desativar a conta de convidado após o tempo previamente estabelecido pela biblioteca);
b) Dependendo da configuração de fábrica do computador, poderá haver máquinas com sistema operacional Linux ou Windows;
c) Manter instalados e atualizados o sistema operacional, os antivírus e os navegadores de Internet;
d) É permitido o acesso a sites que não pertençam ao domínio da Universidade, desde que respeitadas as condições de segurança da informação adotadas pelo Sistema de Bibliotecas e pela instituição, tendo em vista as orientações apresentadas na POSIC (UNIVERSIDADE FEDERAL DO CEARÁ, 2013).

Com relação ao acesso à rede Wi-Fi nas bibliotecas, ressalta-se que a STI da Universidade dispunha de um portal e aplicativo já padronizado, mediante *login* e senha, em alguns setores da instituição, e também em duas das 14 bibliotecas visitadas. Após a aplicação da pesquisa e consequente análise dos relatórios, constatou-se que essa seria a forma mais

segura de se padronizar o acesso à Internet sem fio, apesar de haver algumas resistências e contestações, por parte de usuários e de bibliotecários. A restrição do acesso à rede Wi-Fi foi necessária tendo em vista a própria qualidade do sinal, além das ameaças iminentes à que permanece exposta. Assim, ficaram estabelecidas as seguintes diretrizes:

a) O acesso à rede Wi-Fi no Sistema de Bibliotecas é padronizado por meio do portal e aplicativo desenvolvido pela STI da instituição;
b) Os usuários com vínculo institucional têm acesso ao Wi-Fi por meio do número de seu CPF e sua senha do SIGAA;
c) Os usuários que não tenham vínculo com a instituição, ou seja, público externo, visitantes, ensino à distância, projetos de extensão da Universidade ou funcionários terceirizados, deverão recorrer ao cadastro temporário como convidado no próprio portal ou aplicativo da STI (o cadastro de convidados está condicionado ao preenchimento de informações sobre o usuário a ser cadastrado e poderá ser feito por qualquer usuário com vínculo institucional, o qual se responsabilizará pelo acesso de terceiros que estejam vinculados a seu CPF);
d) Os serviços oferecidos pelo portal desenvolvido pela STI, de acordo com a sua política de uso, estão subordinados às regras estabelecidas pelos respectivos provedores e pela Universidade.

Com o objetivo de alinhar essas diretrizes com a POSIC (UNIVERSIDADE FEDERAL DO CEARÁ, 2013), a comissão de bibliotecários que fez parte deste trabalho traçou como meta a continuação da composição da PSI, já estruturada pela Universidade desde 2011, mas com consideráveis atualizações a serem feitas. Em parceria com a STI, a atuação dos bibliotecários será de fundamental importância para contemplar as BUs, com a finalidade de estender as boas práticas documentadas nas diretrizes e também contribuir com o setor de TI, para reforçar que algumas das recomendações supracitadas constem formalmente na PSI da instituição, sendo discutidas, aperfeiçoadas e consolidadas em sua estrutura.

Nesse sentido, a POSIC é composta por: referências normativas; campo de aplicação; introdução; escopo; conceitos e definições; princípios; diretrizes gerais, que contemplam o tratamento dos ativos, o controle de acesso, a auditoria e conformidade e a gestão de continuidade e de riscos; competências e responsabilidades, atribuídas à autoridade máxima, ao comitê gestor de segurança da informação e comunicação, ao dirigente do Departamento de Segurança da Informação e Comunicação (DSIC), bem como ao próprio departamento, e aos membros da instituição, dentre eles, as BUs. Além disso, as penalidades, sanções, período de atualização e o histórico de alterações na política também estão dispostos na POSIC, documento norteador no desenvolvido da PSI para o Sistema de Bibliotecas.

O ideal é que esse modelo de PSI, voltado para as necessidades das BUs, seja elaborado por uma equipe de profissionais da área de TI, em parceria com os bibliotecários e demais profissionais que puderem contribuir com a sua visão de funcionamento dos setores, para que, assim, auxiliem na construção de uma PSI bem delineada e com base em suas necessidades

organizacionais, além de ser definida pelo mais alto nível da organização e aprovada por cada direção.

A PSI, em sua forma mais geral, deve levar em consideração os requisitos da estratégia de negócio, regulamentações e legislação, além do ambiente de riscos e ameaças à segurança da informação, realizando o diagnóstico da situação atual e elaborando um prognóstico. Além disso, deve conter as definições de segurança da informação, quais são os seus objetivos e os princípios básicos para orientar todas as atividades relacionadas à segurança da informação. A PSI ainda deve conter a categorização de seu público, a atribuição de responsabilidades gerais e específicas, de forma que vise ao gerenciamento da segurança da informação, e os processos de tratamento dos desvios e exceções, que devem estar previstos em um plano de contingência.

É preciso que a elaboração do documento seja numa linguagem acessível, clara, simples e direta, sem entrar em detalhes técnicos, a fim de que todos os usuários e colaboradores internos e público externo possam compreendê-la. Inclusive, a PSI pode ser apoiada por políticas específicas do tema (nesse caso, as BUs), detalhadas de tal maneira a considerar as necessidades específicas dos usuários, assim como o interesse da organização. Alguns exemplos disso já foram citados nas diretrizes apresentadas anteriormente, mas é preciso salientar que ações como o controle de acesso, a segurança física do ambiente, a política de *backup* e de senhas, de identificação pessoal, dentre outras, podem e devem ser aplicadas.

É importante ressaltar, ainda, que a PSI deve ser amplamente divulgada e comunicada a todos os usuários, diretores, prestadores de serviço, bolsistas, estagiários, colaboradores, funcionários, público externo, entre outros, de forma que essa informação esteja acessível e visível para todos. Ademais, deve figurar em programas de educação de usuários e educação corporativa, com a finalidade de sensibilizar a todos e chamar a atenção para a questão da importância da segurança da informação.

Com relação às sanções e penalidades, estas não podem estar de fora de uma PSI, afinal, a criação de diretrizes, normas e regras exige isso, pois nem sempre as pessoas envolvidas colaboram ou as seguem, e, nessas situações, devem ser aplicadas sempre que as políticas preestabelecidas forem desrespeitadas.

Contudo, não basta apenas elaborar e estabelecer uma PSI, pois o documento pode e deve passar por revisões e modificações sistemáticas e periódicas, ou sempre que houver necessidade, visando à avaliação de oportunidades, prevenção de riscos, mudanças organizacionais no ambiente de trabalho, condições legais, o surgimento de novas tecnologias, dentre outros fatores. Tudo isso com o intuito de se fazer uma análise crítica e avaliar essas políticas, e isso deve ficar a cargo do gestor máximo e/ou do comitê gestor da PSI. Em suma, faz-se necessário saber adequar a PSI à realidade da instituição, o que garante o sucesso de sua implantação, principalmente quando o bibliotecário traz para si mais esta responsabilidade.

5 CONSIDERAÇÕES PARCIAIS

Sabendo-se que é papel do bibliotecário gerenciar os recursos informacionais disponíveis na biblioteca, bem como solucionar os problemas de sua unidade de informação, esse profissional deve estar atento às novas demandas e preparado para lidar com a gestão de riscos em segurança da informação, indo além da preocupação com a manutenção de computadores. De fato, também é papel da biblioteca monitorar o bom funcionamento de seus equipamentos e, se houver a necessidade, repassar as demandas para o setor competente, mas apenas isso não se constitui como segurança da informação, embora seja parte integrante de uma série de ações e boas práticas.

Concluindo, parcialmente, a discussão sobre o tema, é sabido que a construção de uma PSI já se constitui num grande desafio. Desafio ainda maior é elaborar uma PSI própria para as bibliotecas, ou até mesmo incluir o universo das BUs na PSI da instituição. Os gestores das BUs devem ter em mente que essas políticas, via de regra, são consolidadas num documento geral, que é a própria PSI em nível institucional. Apesar de, muitas vezes, ser focada na área de TI, o ideal é que a PSI contemple todos os aspectos de segurança da informação de maneira organizacional, até mesmo para aqueles que não estão diretamente envolvidos com recursos computacionais.

Diante do exposto, no atual cenário que se configura, as BUs devem ter como uma de suas prioridades a implantação e/ou a inclusão de diretrizes documentadas numa PSI, com a finalidade de atender às Normas Internacionais de Segurança da Informação, e que, ao mesmo tempo, comtemplem as particularidades e necessidades de um ambiente de pesquisa acadêmica, respeitando, evidentemente, os direitos e a liberdade dos usuários, assim como deve respeitar a realidade de cada biblioteca, além de ir ao encontro do PDI da Instituição de Ensino Superior à qual pertence. Aliado a isso, é de suma importância padronizar e criar normas de utilização dos computadores destinados à pesquisa e aos catálogos automatizados, sem prejuízos ou restrições extremas desnecessárias que comprometam o desempenho da comunidade acadêmica à qual a biblioteca atende.

Evidentemente, a discussão sobre essa temática poderá e deverá ser mais explorada na área de Biblioteconomia e Ciência da Informação, principalmente pelo fato de que alguns profissionais já trabalham com isso ou possuem afinidade com o tema. Além disso, há aqueles profissionais que defendem que não haverá qualquer tipo de restrição aplicada aos seus usuários e à sua equipe de trabalho; por conseguinte, pouco ou nenhum controle de segurança da informação. Ainda assim, espera-se ter contribuído sobremaneira para o debate a fim de que novas ideias, discussões e soluções floresçam nesse campo.

REFERÊNCIAS

APPOLINÁRIO, Fabio. **Dicionário de metodologia científica**: um guia para a produção do conhecimento científico. São Paulo: Atlas, 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Coleção ABNT**. Rio de Janeiro, 2014. Disponível em: <http://www.abntcolecao.com.br/ufc/grid.aspx> . Acesso em: 22 nov. 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001**: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro, 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002**: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013b.

BARCELO, Marta; HERZOG, P. **OSSTMM 3.0**: open-source security testing methodology manual. Nebraska: Institute for Security and Open Methodologies, 2010. Disponível em: <http://scadahacker.com/library/Documents/Assessment_Guidance/OSSTMM-3.0.pdf>. Acesso em: 10 fev. 2014.

BARDIN, Lawrence. **Análise de conteúdo**. Lisboa: Edições 70, 1997. 176 p.

BARROS, Aidil Jesus Paes de; LEHFELD, Neide Aparecida de S. **Fundamentos de metodologia**: um guia para a iniciação científica. 2. ed. São Paulo: Makron Books, 2000.

BISHOP, Matt. **Computer security**: art and science. Boston: Addison-Wesley, c2003. 968 p. Disponível em: <http://pt.scribd.com/doc/252378968/Computer-Security-Arts-and-Science-by-Matt-Bishop>. Acesso em: 24 dez. 2016. Erratas e materiais adicionais disponíveis em: <http://nob.cs.ucdavis.edu/book/book-aands/>.

BISHOP, Matt. **Introduction to computer security**. Boston: Addison-Wesley, c2005. 747 p. Disponível em: <http://www.uoitc.edu.iq/images/documents/informatics-institute/exam_materials/Introduction%20to%20Computer%20Security%20pdf%20DONE.pdf>. Acesso em: 24 dez. 2016.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, DF: Presidência da República. Casa Civil, 14 jun. 2000. p. 2. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 20 dez. 2016.

BRASIL. Decreto nº 5.903, de 20 de setembro de 2006. Regulamenta a Lei nº 10.962, de 11 de outubro de 2004, e a Lei nº 8.078, de 11 de setembro de 1990. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 21 set. 2006. p. 4.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da

Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 18 nov. 2011. Edição Extra, p. 1.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 dez. 2016.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **GSI realiza 5ª Reunião Ordinária do CGSI/2016**. Brasília, 2016. Disponível em: <http://dsic.planalto.gov.br/noticias/521-gsi-realiza-5-reuniao-ordinaria-do-cgsi-2016>. Acesso em: 22 dez. 2016.

BRASIL. Superior Tribunal de Justiça. Secretaria de Controle Interno. Coordenadoria de Auditoria de Tecnologia da Informação. **Cartilha de Segurança da Informação**. Brasília, [2014]. Disponível em: <http://www.stj.jus.br/portal_stj/arquivos/cartilha.pdf>. Acesso em: 10 fev. 2014.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 2. ed. Brasília, 2007. 70 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF>. Acesso em: 10 fev. 2014.

BRASIL. Tribunal de Contas da União. **Cartilha de segurança da informação**. 4. ed. Brasília, 2012. 103 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF>. Acesso em: 10 fev. 2014.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Cartilha de segurança para internet**. 2. ed. São Paulo: CGI.br, 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 dez. 2016.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Neutralidade da rede no marco civil da Internet**. [2016]. Disponível em: <http://marcocivil.cgi.br/contribution/neutralidade-da-rede-no-marco-civil-da-internet/139>. Acesso em: 29 dez. 2016.

CONCERINO, Arthur José. Internet e segurança são compatíveis? In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.). **Direito & internet***:* aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005. cap. 4.

ELLIOT, John. **La investigación-acción en educación**. Tradução de Pablo Manzano. 3. ed. Madrid: Morata, 1997. Disponível em: <http://goo.gl/vGU2wz>. Acesso em: 25 ago. 2016.

GONZAGA, Luiz. **Noções básicas de segurança da informação**. Fortaleza, 2014. 126 slides.

GUELMAN, Luiz. **Conscientização de usuários***:* como envolver seu público com a segurança da informação. In: MÓDULO SOLUTIONS FOR GRC. 08 ago. 2006. Disponível em: <http://www.modulo.com.br/comunidade/entrevistas/616-conscientizacao-de-usuarios-como-envolver-seu-publico-com-a-seguranca-da-informacao>. Acesso em: 15 dez. 2014.

IGLESIAS, María Elinor Dulzaides; GÓMEZ, Ana María Molina. Análisis documental y de información: dos componentes de un mismo proceso. **ACIMED**, Ciudad de La Habana, v. 12, n. 2, p. 1-5, mar./abr. 2004. Disponível em: <http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000200011&lng=es&nrm=iso>. Acesso em: 26 ago. 2016.

INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS (IFLA). UNITED NATION EDUCATION, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO). **Diretrizes para o manifesto IFLA/UNESCO sobre a internet**. [Endossado pelo Conselho Diretor da IFLA em agosto de 2014 e atualizado (tradução em língua portuguesa) em novembro de 2014]. [Edinburgh], 2006. Disponível em: <http://www.ifla.org/files/assets/faife/publications/policy-documents/internet-manifesto-guidelines-pt.pdf>. Acesso em: 26 nov. 2014.

JOÃO, Belmiro. Segurança em sistemas de informação. In: _____. **Sistemas de informação**. São Paulo: Pearson, 2012. p. 58-70.

MANDARINO JÚNIOR, Raphael. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010.

NAZARENO, Claudio. Entendendo as polêmicas e as mudanças trazidas pelo Marco Civil da Internet. In: CÂMARA DOS DEPUTADOS. Centro de Documentação e Informação. **Marco Civil da internet**. Brasília, DF: Edições Câmara, 2014. p. 9-27.

NUNAN, David. **Research methods in language learning**. Cambridge: Cambridge University Press, 1997.

OLIVEIRA, Maria Marly de. **Como fazer pesquisa qualitativa**. Petrópolis: Vozes, 2007.

SOBRAL, Fábio. Segurança da Informação: como garantir a confiabilidade e a integridade? **Biblioo**: cultura informacional, 5 mar. 2012. Disponível em: <http://biblioo.info/seguranca-da-informacao>. Acesso em: 10 fev. 2014.

REZENDE, Denis Alcides; ABREU, Aline França de. **Tecnologia da informação aplicada a sistemas de informação empresariais**: o papel estratégico da informação e dos sistemas de informação nas empresas. 3. ed. rev. e ampl. São Paulo: Atlas, 2003.

UNIVERSIDADE FEDERAL DO CEARÁ (UFC). **Plano de Desenvolvimento Institucional (PDI)**: 2013-2017. Fortaleza, 2012. p. 128, item 3. Disponível em: <http://www.ufc.br/images/_files/a_universidade/plano_desenvolvimento_institucional/pdi_ufc_2013-2017.pdf>. Acesso em: 22 abr. 2016.

UNIVERSIDADE FEDERAL DO CEARÁ (UFC). **Política de Segurança da Informação e Comunicação – POSIC**. Fortaleza, 2013. Disponível em: <http://www.sti.ufc.br/wp-content/uploads/2016/08/politica-seguranca-informacao-ufc.pdf>. Acesso em: 22 abr. 2016.

UNIVERSIDADE FEDERAL DO CEARÁ (UFC). Biblioteca Universitária (Comissão de Serviços). **Diretrizes para uso e manutenção dos computadores destinados aos usuários do Sistema de Bibliotecas da Universidade Federal do Ceará**. Fortaleza, 2015a. Disponível em: <http://www.biblioteca.ufc.br/images/arquivos/normativos/diretriz_uso_computadores_usuarios.pdf>. Acesso em: 20 abr. 2016.

UNIVERSIDADE FEDERAL DO CEARÁ(UFC). Biblioteca Universitária (Comissão de Serviços). **Diretrizes para o acesso à Internet sem fio (rede Wi-Fi) nas dependências do Sistema de Bibliotecas da Universidade Federal do Ceará**. Fortaleza, 2015b. Disponível em: <http://www.biblioteca.ufc.br/images/arquivos/normativos/diretriz_acesso_wifi.pdf>. Acesso em: 20 abr. 2016.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. São Paulo: Atlas, 2000.

VIEIRA, Tatiana Malta. **Compilação de Legislação específica relacionada à segurança da informação (atualizada até 14 de agosto de 2014)**. Revisor Josemar Andrade Fraga. Brasília, DF: Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR), 2014. Disponível em: <http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm>. Acesso em: 20 dez. 2016.

WEB ANEXO TECHNOLOGY. **Segurança da informação**. Criado em 20 jul. 2011. Disponível em: <http://www.anexotechnology.com.br/projetos_seginfo.html>. Acesso em: 10 dez. 2014.

AGRADECIMENTOS

Os autores agradecem aos bibliotecários: Ana Elizabeth Albuquerque Maia; Ericson Bezerra Viana; José Jairo Viana de Sousa; Kalline Yasmin Soares Feitosa; Mara Roxanne de Souza Santos e Vanessa Pimenta Rodrigues Simões. Agradecem ao Professor Edson Alencar e à Professora Elzenir Coelho pela revisão e tradução do artigo. Agradecem também às diretoras das 14 bibliotecas da UFC, que gentilmente contribuíram nas respostas ao formulário de pesquisa.

[i] Conforme o panorama geral apresentado de forma concisa no quadro 1, foram inseridas as áreas do conhecimento contempladas pelo Sistema de Bibliotecas da UFC. A divisão por área foi a mais próxima possível aos cursos presentes nos *campi* a que as bibliotecas atendem; por isso, poderá haver mais de uma área do conhecimento especificada para cada grupo de bibliotecas. Para maior detalhamento das condições encontradas em cada biblioteca, há um quadro mais completo que pode ser consultado nos documentos suplementares deste artigo.

10.20396/rdbci.v0i0.8646416