CONSIDERAÇÕES SOBRE A IMPORTÂNCIA DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS

Bruno Pacheco Coelho Leite (UFES) - brunopcleite@gmail.com

Resumo:

Esse artigo traz os conceitos de Engenharia Social, as estratégias de ataques utilizadas pelos engenheiros sociais e os tipos de ameaças e vulnerabilidades que podem ser exploradas por esses indivíduos. Além disso, relata quais ações são necessárias para o estabelecimento de uma segurança da informação efetiva. Detalha o que vem a ser uma Política de Segurança da Informação e os procedimentos necessários para dar ciência aos funcionários sobre a sua existência. Apresenta um estudo de caso sobre a Política de Segurança da Informação nas bibliotecas do Instituto Federal do Espírito Santo. Informa sobre as melhores maneiras para prevenir possíveis perdas, danos e destruição das informações presentes nessas unidades de informação. Os procedimentos utilizados para este estudo se alicerçam na realização de pesquisa bibliográfica constituída por livros e artigos científicos pertinentes ao tema proposto. Assim, busca analisar os efeitos de uma Política de Segurança da Informação nas Bibliotecas do referido instituto, destacando-se os aspectos ligados a fatores humanos. Além disso, a pesquisa teve como objetivos específicos levantar informações sobre a engenharia social, identificar os tipos de ameaças e vulnerabilidades que contribuem para a ação dos engenheiros sociais nessas bibliotecas e apresentar os propósitos de uma Política de Segurança da Informação. Os resultados obtidos a partir desse estudo poderão ser úteis para bibliotecas que apresentam características semelhantes e estão inseridas em instituições com realidades similares.

Palavras-chave: *Segurança da informação; Engenharia social; Bibliotecas.*

Área temática: *Eixo 1 - Gestão sustentável*

Subárea temática: *Políticas Institucionais*

1 Introdução

Esse estudo[1] traz uma proposta de visão que vá além de investimentos centrados em segurança física e tecnológica, mas que se atente para os aspectos ligados a segurança humana, considerada o elemento mais frágil dentro de uma organização.

Diante do imenso volume informacional gerado diariamente, as bibliotecas atentaram-se para a adoção das tecnologias de informação e comunicação com o intuito de aperfeiçoar a prestação de seus serviços. A partir dos avanços tecnológicos foi possível proporcionar uma prática moderna de gestão para os bibliotecários. Além disso, contribuiu para que essas unidades de informação ofertassem seus serviços para além de suas estruturas físicas.

A oferta de novos serviços advindos do uso das tecnologias da informação trouxe questionamentos quanto aos aspectos relacionados à salvaguarda de suas informações. Através dessas indagações a segurança da informação tem se mostrado como algo que tem preocupado muito as organizações. Deve-se a isso a complexidade de estabelecerem-se metodologias que garantam a proteção das informações por completo.

Conforme vão sendo estabelecidas as melhores práticas para a segurança da informação, também são desenvolvidas táticas para burlá-las. Dessa forma, é preciso ter ciência de que a segurança da informação não contempla somente investimentos em ativos físicos e tecnológicos, é preciso acompanhar a contribuição dos recursos humanos na exposição dessas informações e como os engenheiros sociais se aproveitam dessas vulnerabilidades.

O estabelecimento de uma Política de Segurança da Informação tem o papel fundamental de divulgar a filosofia da empresa em relação à segurança da informação e direcionar as ações a serem tomadas pelos seus funcionários em situações de ameaças.

A atenção desse estudo está voltada para medidas que garantam a segurança da informação nessas unidades de informação, tendo em vista o grande fluxo de pessoas que passam diariamente por esses locais. Para tanto, essa pesquisa levanta informações sobre a engenharia social, e realiza um estudo de caso que visa mostrar os tipos de ameaças e vulnerabilidades que contribuem para a ação dos engenheiros sociais nessas bibliotecas. Além disso, apresenta os propósitos de uma Política de Segurança da Informação.

2 Revisão de literatura

Essa seção apresenta uma revisão de literatura pertinente aos temas abordados nesse estudo, na qual subsidia às análises e discussões frente aos dados coletados no marco empírico.

2.1 Engenharia social e estratégias de ataque

De acordo com Fontes (2006, p. 120) o termo Engenharia Social refere-se ao "[...] conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade". Por sua vez, um dos precursores e especialista na área, Mitnick (2003, p. 6) diz que a Engenharia Social "usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na

[1] Apresenta recortes pertencentes a um trabalho de conclusão de curso de Pós-Graduação *lato sensu* (Gestão Estratégica da Tecnologia) submetido à Universidade Gama Filho, intitulado como "Política de segurança da informação: estudo de caso das bibliotecas do Ifes".

verdade ele não é, ou pela manipulação". E complementa dizendo que como resultado, obtêm-se informações com ou sem o uso de recursos tecnológicos.

O engenheiro social consegue analisar o contexto em que se encontra a informação desejada e espera até que a melhor oportunidade para a obter apareça. Não há um horário e dia estabelecido para o ataque, ele aguarda o melhor momento para montar o cenário, seja através de um encontro ou uma simples conversa. A partir do enredo criado ele consegue retirar as informações sem que suas vítimas notem que estão sendo manipuladas para essa finalidade (SILVA et al., 2012).

Nessa perspectiva, considera-se a Engenharia Social como uma forma de ataque, onde o atacante consegue cativar pessoas e assim obter as informações desejadas sem que suas vítimas percebam. Sendo assim, percebe-se a importância de se estabelecer procedimentos que previnam a ação desses indivíduos em bibliotecas, tendo em vista a movimentação constante de pessoas em busca de informações que atendam às suas necessidades. Entretanto, é possível que pessoas mal-intencionadas obtenham informações privilegiadas, que cabem somente aos bibliotecários conhecê-las.

O engenheiro social beneficia-se da simpatia e do poder de convencimento para acessar as informações pretendidas. Assim, ao comunicar-se com algum empregado de determinada instituição utilizar-se-á de alguns artifícios para envolver a vítima. Silva (2012) relata que o encantamento por parte do contratado pelo novo emprego pode favorecer o ataque do engenheiro social, tendo em vista sua dedicação e a vontade em mostrar-se disponível em ajudar. Nesse caso, o novo funcionário deve ser instruído a respeito de como agir no trabalho e saber lidar em situações de ameaças, para que não se torne alvo de ação do engenheiro social.

Ao conhecer os meios utilizados pelo engenheiro social em seus ataques, torna-se possível que as organizações se previnam contra possíveis investidas junto as suas informações. Além disso, devem atentar-se para o comportamento de seus empregados, principalmente para aqueles que de alguma forma demonstram descontentamento, pois os mesmos, através de alguma motivação, poderão adulterar informações preciosas ou até mesmo fornecê-las para pessoas mal-intencionadas.

2.2 Ameaças e vulnerabilidades

De acordo com Sêmola (2003), as ameaças constituem-se em agentes ou condições que são responsáveis por danificarem e comprometerem as informações e seus ativos por meio da exploração de vulnerabilidades. Ou seja, são situações em que se corre o risco de perdas informacionais por meio de alguma vulnerabilidade existente. Sendo assim, Peixoto (2006) classifica as ameaças em relação a sua intencionalidade, dividindo-as em grupos, a saber:

- **Ameaças naturais** – Ligadas aos fenômenos da natureza;
- **Ameaças involuntárias** – Na maioria das vezes são causadas por erros, acidentes, falta de energia entre outros. São inconscientes e suas causas geralmente estão ligadas ao desconhecimento;
- **Ameaças voluntárias** – Associam-se a Engenharia Social. Ocorrem pela ação de seres humanos como *hackers*, invasores, espiões, ladrões, disseminadores de vírus de computador, incendiários e são causadas de forma proposital (PEIXOTO, 2006, p. 43).

Já no que se refere às vulnerabilidades, Sêmola (2003) afirma ser a representação de uma fragilidade, que ao ser explorada por ameaças, permite a ocorrência de um incidente, afetando as características das informações. A partir dessa ideia tem-se que somente as

vulnerabilidades não geram incidentes, sendo preciso um agente causador ou condições favoráveis (ameaças) para que essa situação ocorra.

Os exemplos de vulnerabilidades expostas por Sêmola (2003) são as seguintes:

> - **Físicas** – Instalações prediais mal elaboradas; falta de mecanismos para combater incêndios; riscos de explosões;
> - **Naturais** – Desastres naturais, como enchentes, terremotos, tempestades, e outros, como falta de energia, acúmulo de poeira, aumento de umidade e de temperatura que podem danificar ou causar mau funcionamento dos computadores;
> - ***Hardware*** – Falha no funcionamento dos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros decorrentes da instalação;
> - ***Software*** – Problemas provenientes de erros ao executar a instalação ou na configuração, que trazem como consequência, acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade do recurso quando necessário;
> - **Mídias** – CD's, DVD's, fitas, entre outros, podem ser perdidos ou avariados. A radiação eletromagnética pode estragar diversos tipos de mídias magnéticas;
> - **Comunicação** – Acessos a locais em que não há permissão ou perda de comunicação;
> - **Humanas** – Falta de treinamento de pessoal, vazamento de informações confidenciais, falta de aplicações das rotinas de segurança, erros ou omissões; ameaças terroristas, sabotagens, greves, vandalismo, roubo, destruição da propriedade ou dados, invasões ou guerras (SÊMOLA, 2003, p. 48-49).

A descrição das particularidades de cada um dos termos acima contribui para a compreensão de como essas condições/fragilidades comportam-se no contexto organizacional. É importante ressaltar que nas duas ocasiões há a presença do fator humano como agente causador de algum incidente que comprometa as propriedades pertencentes às informações.

2.3 Segurança da informação

O termo segurança envolve todas as ações praticadas junto às políticas, aos procedimentos e às medidas técnicas para causar o impedimento de acesso não autorizado, alterações, roubos ou danos físicos aos sistemas de informação (LAUDON; LAUDON, 2011).

No que tange à informação, Sêmola (2003, p. 45) afirma ser como um grupo de dados utilizados "para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos".

Algumas medidas de segurança são estabelecidas para que a proteção da informação seja efetuada de forma objetiva, prevenindo-se contra a ocorrência de incidentes. Para isso, são utilizadas práticas, procedimentos e mecanismos que impeçam que ameaças explorem vulnerabilidades. Conforme Sêmola (2003), essas medidas de segurança controlam o risco de ataque ou limitam o seu impacto e caracterizam-se como:

> - **Preventivas**: medidas de segurança que tem como objetivo evitar que incidentes venham a ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança na instituição. Como exemplos podemos citar as políticas de segurança, instruções e procedimentos de trabalho, especificação de segurança, campanhas e palestras da política de segurança (*firewall*, antivírus, configurações adequadas de roteadores e dos sistemas operacionais etc.);
> - **Detectáveis**: medidas de segurança que visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades. Alguns exemplos são: análise de riscos, sistemas de detecção de intrusão, alertas de segurança; câmeras de vigilância, alarmes, etc.;
> - **Corretivas**: ações voltadas à correção de uma estrutura tecnológica e humana

> para que as mesmas se adaptem às condições de segurança estabelecidas pela instituição, ou voltadas à redução dos impactos: equipes para emergências, restauração de *backup*, plano de continuidade operacional, plano de recuperação de desastres (SÊMOLA, 2003, p. 49).

Aprofundando-se na literatura, Sêmola (2003) considera a Segurança da Informação como uma prática de gestão de riscos de incidentes que garantam a proteção da informação sobre os três princípios básicos que norteiam a implementação dessa prática: confidencialidade, integridade e disponibilidade. Para isso, regras seriam definidas para subsidiarem as ações a serem realizadas sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, favorecendo a identificação e o controle de ameaças e vulnerabilidades.

Proteger a informação segundo Sêmola (2003) significa garantir:

> - **Confidencialidade**: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas;
> - **Integridade**: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais;
> - **Disponibilidade**: Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade (SÊMOLA, 2003, p. 45).

Fontes (2006) ainda acrescenta as seguintes propriedades:

> - **Auditabilidade**: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação;
> - **Não repúdio de autoria**: o usuário que gerou ou alterou a informação (arquivo de texto ou mensagem de correio eletrônico) não pode negar o fato, pois existem mecanismos que garantem sua autoria (FONTES, 2006, p. 12).

Verifica-se ao analisar os princípios acima, que o problema junto às práticas de segurança de informação limita-se a aspectos pertencentes a dois mundos diferentes e por vezes conflitantes: o mundo da tecnologia e o mundo dos seres humanos (SILVA, 2007). Portanto, é preciso que se estabeleçam medidas de proteção que tenham como escopo a segurança física, tecnológica e a humana, sendo esta última a mais complexa, pois envolve características psicológicas, socioculturais, emocionais e outras inerentes ao ser humano, que podem se manifestar de diferentes maneiras conforme a realidade de cada indivíduo.

2.4 Política de segurança da informação

De acordo com Fontes (2006) a política de segurança dispõe para todos os usuários que de algum modo estão em contato com a informação qual é a filosofia da organização sobre esse recurso, com o intuito de garantir que toda a informação da empresa e de seus clientes esteja preservada contra possíveis perdas, danos, destruição e/ou mau uso. Complementando as particularidades do termo, Caruso (2006) especifica que por política de segurança considera-se política gerada, estabelecida e em contínuo processo de revisão, aplicada a todos os níveis da organização, com regras de fácil compreensão e estrutura gerencial e material de apoio a essa política, claramente mantida pela alta hierarquia. Nesse sentido, Sêmola (2003) nos diz que a política deve ser personalizada, devendo-se estipular

padrões, responsabilidade e critérios para o manuseio, armazenamento, transporte e descarte das informações.

É importante ressaltar que de nada adianta o investimento na elaboração de uma política de segurança da informação sem que haja a preocupação em divulgá-la. Essa falta de publicidade tem sido um dos fatores que mais tem contribuído para que a política de segurança da informação se torne ineficaz. Mesmo sendo uma das maiores vilãs, a falta de comunicação não é o único problema presente. É preciso que as organizações personalizem suas ações de defesa conforme o contexto em que seus ambientes se encontram, preocupando-se sempre em revê-las. O objetivo dessa revisão é antecipar-se aos possíveis danos que podem ser causados às informações.

Assim, conforme Caruso (2006) a política de segurança deve conter orientações claras a respeito de alguns aspectos, tais como:

- **Objetivos da segurança**: deve explicar de forma rápida e sucinta a finalidade da política de segurança;
- **A quem se destina**: deve definir claramente quais as estruturas organizacionais e os ocupantes de funções aos quais a política se aplica;
- **Propriedade dos recursos**: deve definir de forma clara as regras que regerão os diversos aspectos relacionados com a propriedade de ativos de informações;
- **Responsabilidades**: deve definir de forma clara quais os tipos de responsabilidades envolvidas com o manuseio de ativos de informações, a quem ele deve ser atribuído e quais os mecanismos de transferência;
- **Requisitos de acesso**: deve indicar de forma clara quais os requisitos a serem atendidos para o acesso a ativos de informações;
- **Responsabilização**: deve indicar as medidas a serem tomadas nos casos de infringência às normas;
- **Generalidades**: nesta seção da política podem ser incluídos os aspectos que não cabem nas demais. Pode-se incluir aqui uma definição dos conceitos envolvidos, um glossário e uma indicação das normas acessórias (CARUSO, 2006, p. 57).

Ao desenvolver uma política de segurança da informação é importante que a organização identifique os principais riscos que tornam suas informações suscetíveis a ataques. Vale lembrar que a política de segurança deverá estabelecer os mecanismos e metas a serem alcançados no que se refere à salvaguarda destas informações, além disso, necessita-se realizar revisões periódicas sobre essas medidas haja vista o aprimoramento das técnicas de ataques.

2.5 Bibliotecas

As bibliotecas se enquadram em diferentes categorias. Suas características variam conforme a faixa etária e os públicos as quais se destinam. As bibliotecas objetos desse estudo atendem desde alunos de ensino médio até alunos de pós-graduação. Dessa forma, possuem características híbridas, tanto de bibliotecas escolares, que tem por objetivo principal a oferta de livros e material didático para alunos e professores, quanto de bibliotecas universitárias, que possuem como foco o fornecimento de infraestrutura bibliográfica e documental aos cursos, pesquisas e serviços ofertados pela instituição onde essas se encontram (FONSECA, 2007).

De acordo com Tarapanoff (1982, apud DRUCKER, 1973), estudos realizados com base na teoria das organizações permitem caracterizar a biblioteca como sendo uma instituição ou organização de serviço sem autonomia própria. Dessa forma, os serviços prestados por ela fornecem assistência bibliográfica e documental às funções de ensino, pesquisa e extensão através da sua principal matéria-prima, a informação.

No que tange a organização das coleções existentes em seus espaços, as bibliotecas podem ser de dois tipos, centralizadas ou descentralizadas/departamentalizadas. São centralizadas quando seus acervos são organizados e gerenciados por uma única direção, ou seja, há uma biblioteca central que dá os comandos para serem executado pelas outras. Já as descentralizadas/departamentalizadas, na qual se enquadram as bibliotecas desse estudo, possuem acervos próprios em cada unidade de ensino da instituição e possuem autonomia nas suas decisões (SILVA; ARAUJO, 2003).

Conforme apresentado acima, por ser tratar de uma organização de serviço próprio sem autonomia, e por ter características de uma organização, necessita-se que a biblioteca disponha de um suporte administrativo que atenda a toda sua estrutura. Para isso, é necessário estabelecer um conjunto de medidas tais como legislação, regulamentação, definição clara dos seus objetivos e responsabilidades, hierarquia, raio de influência, funções/atribuições e coordenação (SILVA; ARAUJO, 2003).

Percebe-se que os bibliotecários exercem tanto as funções técnicas, quanto as informacionais e administrativas. Isto se justifica em razão do contexto complexo em que as organizações estão inseridas atualmente, exigindo habilidades que são desenvolvidas no dia-a-dia, e que possibilitam a esses profissionais analisar e desenvolver soluções para os problemas que envolvam suas bibliotecas (MACIEL; MENDONÇA, 2006).

O Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo – Ifes, possui dezessete *campi* em funcionamento, e outros estão em processo de implantação[2]. Cada *campus* é contemplado por uma biblioteca, que é administrada, em média, por dois bibliotecários. Essas unidades de informação visam atender às necessidades informacionais dos cursos de ensino médio integrados com técnicos, cursos de graduação e pós-graduação.

Através da implantação de um sistema de gerenciamento de bibliotecas, o Pergamum®, os serviços prestados por essas bibliotecas foram aprimorados e como consequência trouxeram agilidade no atendimento e processamento das informações. Porém, a quantidade de pessoas atendidas diariamente é enorme, o que favorece a ocorrência de possíveis falhas na operacionalização desse sistema, tais como alteração e divulgação das informações registradas. Vale ressaltar que a base de dados do sistema Pergamum® é compartilhada, ou seja, todas as bibliotecas do IFES possuem acesso, sendo permitida a manipulação desses dados.

3 Materiais e métodos

Esse trabalho constitui-se de um estudo de caso. O objetivo geral da pesquisa foi analisar os efeitos de uma Política de Segurança da Informação nas Bibliotecas do Ifes destacando-se aspectos ligados a fatores humanos. Além disso, a pesquisa teve como objetivos específicos levantar informações sobre a engenharia social, identificar os tipos de ameaças e vulnerabilidades que contribuem para a ação dos engenheiros sociais nessas bibliotecas e apresentar os propósitos de uma Política de Segurança da Informação.

Para a fundamentação teórica do trabalho foi realizada uma pesquisa bibliográfica com o intuito de auxiliar na investigação dos assuntos pertinentes aos temas centrais desse estudo. Assim, foram utilizados livros, normas e artigos científicos provenientes das áreas de Tecnologia da Informação e Biblioteconomia.

O instrumento utilizado para a obtenção dos dados valeu-se da aplicação de um questionário (QUESTIONÁRIO 1) de autoria própria composto por 15 (quinze) perguntas baseadas na norma ABNT NBR ISO/IEC 27002:2005. Tal ferramenta contribuiu para a evolução desse estudo.

[2] Situação referente ao ano de 2013.

Questionário 1 - Pesquisa sobe Política de Segurança da Informação

Questionário baseado na norma ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação		
Perguntas		**Opções de resposta**
1	Na instituição onde sua biblioteca está inserida há uma política de segurança da informação aprovada pela alta administração, publicada e comunicada?	( ) Sim ( ) Não ( ) Não sei
2	A direção apoia ativamente a segurança da informação, atribuindo e reconhecendo responsabilidades de forma explícita?	( ) Sim ( ) Não ( ) Não sei
3	É realizado um inventário de todos os ativos (físicos, tecnológicos e humanos) atribuindo responsabilidade a um proprietário?	( ) Sim ( ) Não ( ) Não sei
4	Há assinatura de termos que contemplem as responsabilidades dos funcionários em relação à confidencialidade, proteção dos dados, ética, uso apropriado dos recursos e dos equipamentos da organização?	( ) Sim ( ) Não ( ) Não sei
5	Há uma definição de perímetros e controles de acesso físico à biblioteca tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionista?	( ) Sim ( ) Não ( ) Não sei
6	Há procedimentos documentados para atividades como inicialização e desligamento de computadores, geração de cópias de segurança (*backup*), manutenção de equipamentos e tratamento de mídias?	( ) Sim ( ) Não ( ) Não sei
7	O sistema de gerenciamento de biblioteca é alimentado corretamente através da checagem das entradas de dados permanentes (por exemplo, nomes, endereços, telefones dos usuários)?	( ) Sim ( ) Não ( ) Não sei
8	Há um canal de contato que seja de seu conhecimento que esteja sempre disponível e em condições de assegurar uma resposta adequada e oportuna em relação a incidentes de segurança da informação?	( ) Sim ( ) Não ( ) Não sei
9	Há planos desenvolvidos e implementados para a manutenção ou recuperação das operações referentes aos sistemas de gerenciamento de bibliotecas que assegurem a disponibilidade da informação após a ocorrência de interrupções ou falhas?	( ) Sim ( ) Não ( ) Não sei
10	Há um processo ordenado de encerramento de atividades que inclua a devolução de equipamentos e retirada de direitos de acesso?	( ) Sim ( ) Não ( ) Não sei
11	Há treinamento apropriado para conscientização da importância de mecanismos para a segurança da informação?	( ) Sim ( ) Não ( ) Não sei
12	Na biblioteca onde atua há segregação de funções e ambientes?	( ) Sim ( ) Não ( ) Não sei
13	Há políticas, procedimentos e controles para proteger a troca de informações em todos os recursos de comunicação (inclusive correio eletrônico, telefone e sistemas de informação)?	( ) Sim ( ) Não ( ) Não sei
14	Os servidores e usuários da biblioteca são orientados a seguir boas práticas de segurança da informação na seleção e uso de senhas?	( ) Sim ( ) Não ( ) Não sei
15	Há políticas de mesa limpa e tela limpa (sem anotações à mostra)?	( ) Sim ( ) Não ( ) Não sei

Fonte: elaborado pelo autor.

A coleta dos dados ocorreu através da aplicação de questionário em formato eletrônico. A proposta era de que pelo menos um representante (bibliotecário) de cada biblioteca respondesse. Dessa forma, os entrevistados tiveram o prazo de uma semana para responder as questões. Das dezessete bibliotecas para as quais o questionário foi encaminhado, conseguiu-se a resposta de dez.

4 Resultados finais

Com o intuito de facilitar a apresentação dos dados coletados, optou-se por agrupar os resultados conforme algumas orientações descritas pela norma ABNT NBR ISO/IEC 27002 (2005, p. 8) no que tange a códigos de prática para a gestão da segurança da informação.

- **Política de segurança da informação.** Quando perguntados se há uma política de segurança da informação na instituição, somente 10% dos respondentes afirmaram ter conhecimento de sua existência.
- **Comprometimento da direção com a segurança da informação.** De acordo com os levantamentos, 30% dos entrevistados afirmaram que a direção apoia ativamente a segurança da informação, atribuindo e reconhecendo responsabilidades de forma explícita.
- **Responsabilidade pelos ativos.** No que tange as propriedades dos recursos, 60% dos bibliotecários afirmam que são efetuados inventários que abranjam todos os ativos da instituição, atribuindo responsabilidades a um proprietário.
- **Segurança em recursos humanos.** Diante das análises, 50% dos entrevistados desconhecem a existência de termos que contemplem as responsabilidades dos funcionários em relação à confidencialidade, proteção de dados, ética e uso apropriado dos recursos e equipamentos.
- **Procedimentos e responsabilidades operacionais.** Somente 20% dos respondentes afirmaram haver procedimentos documentados para atividades como inicialização e desligamento de computadores, geração de cópias de segurança (*backup*), manutenção de equipamentos e tratamento de mídias. A respeito da existência de políticas, procedimentos e controles para proteger a troca de informações em todos os recursos de comunicação, 50% dos entrevistados afirmaram existir.
- **Controle de acessos.** Em relação ao controle de acessos, 70% dos bibliotecários afirmaram haver controles de acesso físico nas bibliotecas, tais como paredes, portões de entrada ou balcões de recepção. Em contrapartida, apenas 30% dizem ocorrer um processo ordenado de encerramento de atividades que inclua a devolução de equipamentos e a retirada de direitos de acesso.
- **Gestão de incidentes de segurança da informação.** Quando perguntados se há um canal de contato que possam consultar que assegure uma resposta adequada e oportuna em relação a incidentes de segurança da informação, 70% dos respondentes afirmam conhecê-lo.
- **Gestão da continuidade do negócio.** Por fim, 50% dos entrevistados afirmam haver planos para a manutenção ou recuperação das operações referentes ao sistema de gerenciamento de biblioteca que assegurem a disponibilidades da informação após a ocorrência de interrupções ou falhas.

Além desses, foi possível compilar outro dado considerado importante para essa pesquisa, onde 90% dos bibliotecários afirmaram não haver um treinamento apropriado para conscientização da importância de mecanismos para a segurança da informação.

5 Considerações finais

A pesquisa realizada mostrou que até o ano de 2013 havia o desconhecimento por parte dos bibliotecários sobre a existência de uma Política de Segurança da Informação que estivesse efetivamente implementada no Ifes.

Foi possível verificar também que nem todas as bibliotecas são contempladas por inventários que atribuam responsabilidades pelos ativos a um responsável, deixando-os vulneráveis para a prática de vandalismo e roubo. Além disso, não está estabelecido em todos os *campi* à assinatura de termos que assegurem responsabilidades em relação à confidencialidade, proteção dos dados, ética e uso apropriado dos equipamentos, permitindo brechas para o vazamento de informações confidenciais, sabotagens e destruição de dados.

A pesquisa mostrou, que embora as bibliotecas façam parte da mesma instituição, não está claro ainda para os bibliotecários, os procedimentos necessários para um relacionamento consciente com as informações. Essa realidade tem relação com a distância geográfica existente entre os *campi*, pois dificulta o acompanhamento de aplicações de rotina. Além disso, cada *campus* possui características próprias de administração, norteadas pela realidade da região onde este está inserido.

É notável, com base nesse estudo, a necessidade de treinamentos que conscientizem a importância de mecanismos que garantam a segurança da informação nessas bibliotecas, pois não há procedimentos que subsidiem às tomadas de decisões relativas ao gerenciamento consciente das informações em situações de ameaças e vulnerabilidades.

O propósito de uma Política de Segurança da Informação, neste caso, visa orientar e apoiar medidas necessárias para a gestão da segurança, estabelecendo padrões conforme a filosofia da organização, abrangendo todas as estruturas do seu organograma. É possível também que essa política seja personalizada conforme a demanda de cada setor.

Os resultados obtidos a partir desse estudo permitem concluir que as informações pertencentes a essas bibliotecas não se encontram seguras. As vulnerabilidades humanas estão presentes e a probabilidade da ocorrência de vazamentos de informações é alta. Esse trabalho contribui para que as bibliotecas com características similares se atentem para a necessidade de realizar ações que contemplem a segurança das suas informações.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISSO/IEC 27002**: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

CARUSO, C. A. A.; STEFFEN, F. D. **Segurança em informática e de informações.** 3. ed. rev. e ampl. São Paulo: Senac São Paulo, 2006.

FONSECA, E. N. da. **Introdução à biblioteconomia**. 2. Ed. Brasília: Briquet de Lemos, 2007.

FONTES, E. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais.** 9. ed. São Paulo: Pearson Prentice Hall, 2011.

MACIEL, A. C.; MENDONÇA, M. A. R. **Bibliotecas como organizações**. 1. ed. rev. Rio de Janeiro: Interciência; Niterói: Intertexto, 2006.

MITNICK, K. D.; SIMON, W. L. **A arte de enganar:** ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Makron Books, 2003.

PEIXOTO, M. C. P. **Engenharia social e segurança da informação:** na gestão corporativa. Rio de Janeiro: Brasport, 2006.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. 1. ed. Rio de Janeiro: Elsevier, 2003.

SILVA, C. S. da et al. Engenharia social: o elo mais frágil da segurança nas empresas. **Revista Eletrônica do Alto Vale do Itajaí**, v. 1, n. 2, dez. 2012. p. 29-40. Disponível em: <http://www.revistas.udesc.br/index.php/reavi/article/viewArticle/2840>. Acesso em: 02/07/2013.

SILVA, D. R. P. da; STEIN, L. M. Segurança da informação: uma reflexão sobre o comportamento humano. **Ciências & Cognição**, v. 10, 2007. p. 46-53. Disponível em: <http://www.cienciasecognicao.org/revista/index.php/cec/article/download/628/410>. Acesso em: 02/07/2013.

SILVA, D. A. da; ARAUJO, I. A. **Auxiliar de biblioteca**: técnicas e práticas para formação profissional. 5. ed. Brasília: Thesaurus, 2003.

SILVA, F. C. C. da; SCHONS, C. H.; RADOS, G. J. V. A gestão de serviços em bibliotecas universitárias: proposta e modelo. **Informação & Informação**, Londrina, v. 11, n. 2, jul./dez. 2006. Disponível em: <http://www.uel.br/revistas/uel/index.php/informacao/article/view/1691>. Acesso em 10/09/2013.

TARAPANOFF, K. A biblioteca universitária como uma organização social. **Estudos Avançados em Biblioteconomia e Ciência da Informação**, Brasília, v. 1, n. 1, 1982. Disponível em: <http://www.brapci.ufpr.br/documento.php?dd0=0000003204&dd1=4c414>. Acesso em 10/09/2013.