POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR PÚBLICA

Izaak Silva Candeias[1], Marcus Túlio Pinheiro de Freitas[2]

[1]UNEB/UDO/Gerência de Informática, icandeias@uneb.br

[2]UNEB/UNEAD/Núcleo de Pós-Graduação e Pesquisa, mtpinheiro@uneb.br

Resumo *– Este estudo trata do avanço da importância da informação nas instituições e organizações como principal ativo de nossa sociedade. A metodologia utilizada foi a revisão bibliográfica e documental, com o objetivo de analisar a Gestão do Conhecimento, a Gestão das Instituições de Ensino Superior e as melhoras práticas e normas na área de Segurança da Informação, a serem aplicadas na Universidade do Estado da Bahia. Tendo como finalidade desenvolver uma proposta de uma Política de Segurança da Informação, observando os princípios da Organização Internacional de Normalização, representado no Brasil pela Associação Brasileira de Normas Técnicas, juntamente com a legislação do Estado da Bahia e o regimento da Uneb, preceitos indispensáveis para criação das normas e regulamentos e definir padrões a serem adotados pelos usuários da informação da universidade. Atingidos estes objetivos, será possível constatar a relevância e aplicabilidade desta proposta: disponibilizar, a partir do Comitê Gestor de Segurança da Informação, formado pelos setores estratégicos, um recurso essencial para a proteção da informação, possibilitando uma melhor compreensão do valor da informação no âmbito acadêmico e administrativo, estabelecendo um elo entre os diversos setores e unidades, fomentando a mudança cultural e, ao mesmo tempo, iniciando um processo de socialização e difusão do conhecimento das TICs.*

Palavras-chave: Segurança da Informação. Instituição de Ensino Superior. Tecnologia da Informação e Comunicação. Educação Digital.

Abstract *– This study deals with the advance of the importance of information in institutions and organizations as the main asset of our society. The methodology used was the bibliographical and documentary review, with the objective of analyzing the Knowledge Management, Management of Higher Education Institutions and the best practices and norms in the Information Security area, to be applied at the State University of Bahia. With the purpose of developing a proposal for an Information Security Policy, observing the principles of the International Organization for Standardization, represented in Brazil by the Brazilian Association of Technical Standards, together with the legislation of the State of Bahia and the Uneb regiment, indispensable precepts for the creation of norms and regulations and defines standards to be adopted by information users of university. Having reached these objectives, it was possible to verify the relevance and applicability of this proposal: to provide, from the Information Security Management Committee, formed by the strategic sectors, an essential resource for the protection of information, enabling a better understanding of the value of information in the scope academic and administrative, establishing a link between the various sectors and units, fostering cultural change and, at the same time, initiating a process of socialization and diffusion of ICT knowledge.*

Keywords: Information Security. Higher Education Institution. Information and Communication Technology. Digital education.

1. INTRODUÇÃO

Como seria o mundo sem regras, normas e leis? As leis e os regulamentos servem para dar limites às pessoas e conscientizar sobre seus atos, ou seja, saber o que é certo e errado. E sem elas o mundo estaria uma desordem e completamente devastado. Nos dias atuais é improvável viver sem regras, sem lei e para que seja feita justiça tem de haver normas e valores que nos mostrem o melhor caminho a seguir. Estas são criadas pela e para a sociedade. São validadas e examinadas por um organismo reconhecido e refletem o consenso da instituição, sobre um determinado tema, em um dado momento da história. São evolutivas e o gatilho de uma revisão deve ser a necessidade da própria sociedade (BATTAGIN, 2016).

As políticas de segurança da informação são, de modo geral, expressas como códigos de conduta aos quais os usuários dos sistemas computacionais devem se adaptar inteiramente. Porém, não se vê um debate adequado sobre o grau de aceitação dos usuários a estas políticas, nem se expõem questões sobre o impacto, usualmente considerável, por elas causado sobre o ambiente e sobre o comportamento daqueles que as devem seguir. Quando o tema segurança é tratado, as pessoas relacionam o assunto a invasões por hackers e vulnerabilidades em sistemas, onde a compreensão básica é de que a organização necessita de um bom antivírus, um firewall e ter todos os seus “patches” aplicados no ambiente tecnológico. Não há dúvida de que são questões importantes, porém a Segurança da Informação (SI) não está limitada a somente esses pontos. Não adianta fazer investimentos em tecnologias de última geração e deixar de lado o fator humano. Já que o elo mais fraco na segurança da informação são as pessoas, estas devem ter um foco maior na tentativa de conscientizá-las do destaque que elas têm nesse quesito, afirmam Campos e Prado (2013). Portanto, há uma necessidade muito grande de capacitar os usuários, principalmente os mais novos, recém-admitidos, nos conceitos e boas práticas de segurança, evitando assim os maus hábitos no mundo virtual.

A Educação digital corresponde à conscientização e treinamento das pessoas para o uso das tecnologias, admitindo-lhes desempenho adequado, ético e com a minimização de riscos, assegura Crespo (2010). Diz ainda que educar digitalmente não pode ser simplesmente ensinar a utilizar, na prática, a tecnologia, como o envio de uma mensagem de texto pelo aparelho celular ou de se fazer uma vídeo-chamada entre computadores. É deixar as pessoas aptas diante da fluência de informações e da quantidade excessiva de novos aparelhos eletrônicos, atuar adequadamente.

Marçula (2010) garante que uma forma econômica das instituições atingirem uma segurança mínima é pela educação. Padrões de proteção devem ser disseminados nos campi para que os usuários sejam educados e habilitados para utilização correta da computação. Os usuários devem ser auxiliados para que possam fazer de modo seguro o uso da Internet, fomentando uma cultura de educação digital. O fato de a informação encontrar-se exposta a diversos tipos de ameaças e ataques, seja através de meios físicos, lógicos ou humanos, requer atenção especial, pois as pessoas devem se conscientizar que fazem parte do problema. Toda organização tem que objetivar garantir segurança para o seu principal patrimônio: a informação.

Neste contexto Sousa (2010) diz que a universidade surge como o lócus do conceito de comunidade acadêmica, que se constitui numa relação com o conhecimento como um bem público, aliado à liberdade acadêmica, à esfera pública e à universidade, sendo independente do Estado e do mercado e baseando-se num contrato com a sociedade no qual o Estado providencia o financiamento necessário.

Varela (2008, p. 30) afirma que a universidade busca reforçar o acesso à informação tendo a produção e difusão do conhecimento como algo em comum a todos os acadêmicos e que estrutura vários aspectos da vida acadêmica.

A análise dos temas anteriormente propostos é extremamente pertinente ao âmbito da segurança da informação, uma vez que neste âmbito é comum deparar-se com o seguinte problema: implementam-se regras (genericamente chamadas "políticas") que se mostram inadequadas ao ambiente organizacional, sendo rechaçadas pelos usuários como inadequadas, impraticáveis ou extremamente invasivas. Com o intuito de reduzir esta aversão e de contemplar questões de fato pertinentes, propõe-se a análise do comportamento dos usuários ante a segurança da informação, idealmente em dois momentos, prévia e posteriormente à adoção de tais regras. O atendimento a regras é uma prática social, moldada pelos conceitos inerentes a cada indivíduo e traduzida pelas ações executadas em atendimento, ou não, às regras vigentes. Consequentemente a avaliação do entendimento reside na observação das práticas adotadas, o que atribui um papel extremamente importante à compreensão do lócus de convívio, e que se reflete no conceito de nível de entendimento e o modo de agir social. O grau com que determinada regra é aplicada reflete a sua incorporação pelos indivíduos pertencentes ao contexto social do qual ela emana.

Por mais que a interpretação seja moldada por experiências pessoais, esta representação deve se dar de tal modo que possa ser perceptível de maneira o mais uniforme possível por todos os que devem segui-la, evitando ambiguidades linguísticas e reduzindo os mal-entendidos. Regras devem ser formuladas sem ambiguidade e adequadamente aplicadas, orientam Marciano e Lima-Marques (2006), o que exige, por vezes, elevada carga de julgamentos e percepções, tanto de seus formuladores, quanto daqueles que se espera que as sigam, além de uma prática coerentemente alinhada com a sua formulação. Afirmo, então, que as instituições e organizações podem ser transformadas, e inclusive substancialmente modificadas, pela restruturação de seus componentes.

Devido à falta de formalização de normas de SI na Universidade do Estado da Bahia (UNEB), a situação da infraestrutura de tecnologia chegou a um estado inquietante, pois não se desenvolve da mesma forma que a instituição, embora a equipe de Tecnologia e Informação (TI) se esforce para garantir o bom funcionamento e o atendimento aos usuários, não consegue atingir de forma efetiva os objetivos, devido a nenhuma política de segurança definida. Medidas políticas sobrepõe-se às ações de assunto técnico, o que gera frequentemente vários problemas que afetam à informação em última instância. É imprescindível definir os níveis de acesso, tanto dos dados contidos em nossos servidores quanto dos dados gerados pelos sistemas.

Atuo como gestor do contrato de Suporte e Infraestrutura de Redes na Gerência de Informática (GERINF), setor que está ligado à Unidade de Desenvolvimento Organizacional (UDO) da Uneb. Constato que estamos vulneráveis a vários tipos de ameaças, como físicas, tecnológicas e humanas diariamente e atuamos, sem uma política de acesso ou segurança dos dados, de forma "sob demanda", ou seja, quando as falhas e ameaças aparecem. A Gestão da Segurança da Informação busca o alinhamento entre as necessidades organizacionais de segurança e o gerenciamento dos sistemas de informação (GSIC, 2010). Porém sem uma Política de Segurança da Informação (PSI) formalizada e compartilhada entre a comunidade não teremos uma atuação de qualidade. Precisamos atuar de forma preventiva e não apenas reativa;

favorecer a organicidade e unicidade da universidade. É necessário que medidas de segurança sejam tomadas. Os procedimentos, regras ou normas realmente precisam ser utilizados por todos, independentemente de qual cargo exercem na organização, os usuários precisam conhecer mais detalhadamente tais conceitos para que haja uma aplicação eficaz. Pois, não podemos considerar a informação como um produto final, mas sim, o ponto de partida que leva a um processo de tomada de decisão.

Justifica-se a importância desta pesquisa por ser a característica intrínseca de identificar a oportunidade de transformar o futuro, é o agente que motiva a continuidade e desenvolvimento das Instituições de Ensino Superior (IES) e, portanto, resposta para os anseios da sociedade.

2. REFERENCIAL TEÓRICO

A fundamentação teórica, registrada, a seguir, assinala definições, conceitos e termos procurando reunir as principais investigações conduzidas na área da gestão da SIC. O estudo do estado da arte da segurança dos sistemas de informação será focado nas Diretrizes da SIC (BAHIA, 2011) do Governo do Estado da Bahia, nas boas práticas da SIC, na temática da continuidade do negócio e nos resultados apresentados em artigos científicos sobre o papel do utilizador na segurança dos sistemas de informação. Primeiramente o apoio da Gestão da Informação (GI) e do Conhecimento na seção 2.1 visa maior eficiência na área de Segurança da Informação através do compartilhamento de informações e de ações integradas entre diversos atores, assim como na seção 2.2 a Gestão de Instituições de Ensino Superior (IES) contribui para entender as práticas utilizadas na implantação de PSI em atividades acadêmicas e na percepção de suas particularidades culturais; e por último na seção 2.3 sobre a Segurança da Informação trazendo processos de segurança, estabelecendo objetivos e definindo responsabilidades.

2.1. Gestão da Informação e do Conhecimento

Antes de pensarmos sobre Gestão do Conhecimento (GC), vamos analisar a relação entre dados, informação e conhecimento. Segundo Alavi (2001, p. 111) os dados são fatos, números brutos; as informações são dados processados / interpretados e o conhecimento é informação personalizada. Ela afirma que a GC se concentra em expor os indivíduos a informações potencialmente úteis e facilitar a assimilação de informações.

Como o conhecimento é personalizado, para que o conhecimento de um indivíduo ou de um grupo seja útil para os outros, deve ser expresso de forma a ser interpretável pelos receptores. O armazenamento de informações é de pouco valor; apenas a informação que é processada ativamente na mente de um indivíduo por meio de um processo de reflexão, esclarecimento ou aprendizado pode ser útil (ALAVI, 2001). Se o conhecimento é um processo, então o enfoque de gestão do conhecimento está no fluxo de conhecimento e nos processos de criação, compartilhamento e distribuição de conhecimento. Alavi (2001) fala que a GC possui ainda o objetivo de controlar, facilitar o acesso e manter um gerenciamento integrado sobre as informações em seus diversos meios.

Ao se tratar de dado, informação e conhecimento, o único que é diretamente mensurável é o dado. Ou seja, é o único que pode ser tratado pelos sistemas informatizados é o dado. Os sistemas de informação facilitam os métodos de obtenção de informações com base em uma grande quantidade de dados, e os sistemas de GC

podem ajudar a organizar o conhecimento de uma instituição, contudo, tanto informações quanto conhecimento habitam apenas na mente humana. Valentim (2003) expõe que cada pessoa tem sua forma de “olhar o mundo”, cada organização tem sua própria cultura organizacional. Já para Crozatti (1998), a cultura organizacional é um conjunto de valores e crenças compartilhados que geram certas regras e padrões de comportamento.

De acordo com Chiavenato (2002), uma organização complexa é resultado de um conjunto de partes interdependentes que, unidas, formam um todo, que, por sua vez, é interdependente de um ambiente mais amplo. Caracterizam-se por um elevado grau de complexidade na estrutura e nos processos devido ao grande tamanho (proporções maiores) ou a natureza das operações. Trabalhar a cultura organizacional visando a GC demanda tempo, energia e planejamento. A gestão do conhecimento é um processo dinâmico, não sendo possível definir com exatidão quando o indivíduo está criando conhecimento (tácito), do momento que está socializando (explícito) (VALENTIM, 2003).

Sistemas de Gestão do Conhecimento

Os Sistemas de Gestão do Conhecimento (SGC), conforme Alavi (2001) são recursos de TI que ajudam as ações organizacionais da Gestão do Conhecimento como identificação, concepção, apresentação e difusão do conhecimento dentro do contexto corporativo. A autora ainda argumenta que o objetivo do SGC é apoiar a criação, transferência e aplicação de conhecimento nas organizações.

Alavi (2001) propõe que a tecnologia pode apoiar a aplicação de conhecimentos incorporando o conhecimento em rotinas organizacionais. Procedimentos culturais podem ser incorporados em TI para que os próprios sistemas se tornem exemplos de normas organizacionais. Fazendo-se necessário a compreensão de gestão em IES e o mapeamento dessas rotinas.

2.2. Gestão em Instituições de Ensino Superior

É impraticável ignorar a complexidade das organizações educacionais caso se queira melhor compreender a sua realidade, comportamento e desempenho lembra Meyer Jr (2014). Administrar uma organização acadêmica, cuja missão é educar seres humanos, requer visão, intuição, sensibilidade e o uso de ferramentas administrativas adequadas às especificidades deste tipo de organização.

Tachizawa e Andrade (1999) afirmam que as organizações de modo geral e em particular as IES exigem mais ênfase no gerenciamento do conhecimento e não apenas na administração de dados ou informações. Nesta perspectiva, a abordagem dos autores quanto à necessidade de articulação entre práticas acadêmicas e práticas gerenciais na gestão das universidades, para que sejam impulsionados e captados os aspectos centrais dessas mudanças, parecem esclarecedoras. Salientam também, Tachizawa e Andrade (1999), que o processo de gestão nas IES públicas desenvolve-se levando em consideração a natureza de ação ensino, pesquisa e extensão; a estrutura colegiada para tomada de decisão; e a especificidade dos recursos humanos que compõe o quadro permanente, sejam docentes ou servidores técnico-administrativos, suas crenças e valores.

Meyer Jr (2014) alerta que o fato de inexistir uma teoria própria tem impulsionado os gestores universitários a buscarem conhecimento e práticas utilizadas no setor empresarial, no qual se concentra a essência da teoria

administrativa e no qual a administração é, por excelência, mais praticada, incorporando-as em vários setores e áreas da organização universitária.

Os autores propõem uma administração baseada em evidências alertando aos administradores a buscarem as melhores práticas comprovadamente evidenciadas para suas organizações. As melhores práticas são validadas pelas melhores evidências, reveladas pelas boas práticas e pesquisas sólidas e não pelo modismo. Para Meyer Jr (2014) a ideia de “universidade”, como instituição social, vem se modificando ao longo do tempo. O conceito mais atual revela uma instituição na qual ensino e pesquisa mesclam-se, para responder às demandas sociais e às expectativas de seus inúmeros stakeholders, desempenhando uma função crítica da própria sociedade.

Como Oda (2008) define bem: “... a Organização, etimologicamente, provém do grego “organon” que significa “órgão”, daí atentam-se com os órgãos (empresas, instituições ou entidades), criados pelo homem para o desempenho de certas funções, com vista a atingir fins determinados”. Percebe que há uma combinação de esforços individuais que tem por finalidade realizar propósitos coletivos. Os processos de tomada de decisão na universidade são de forma colegiada e requer conhecimento do funcionamento da gestão universitária, maturidade e capacidade de perceber a relevância do fazer coletivo em detrimento do particular, defende Favero (1999). Assim sendo, os conflitos nela existentes deveriam situar-nos no plano da busca de elementos novos e melhores para a instituição, e não naquele dos interesses pessoais ou das atitudes de dominação e imposição.

Favero (1999) defende que a universidade deve ser entendida como um lócus de pesquisas cientifica e tecnológicas, deve ser também o espaço onde se exerce o pensamento crítico, sem o qual esses avanços procederiam “às cegas”. Sendo, uma das formas pela qual a universidade pode desenvolver o pensamento crítico, segundo a autora, através da formação de profissionais capazes de exercerem papéis especializados em diferentes áreas do conhecimento. Tal formação deverá efetivar-se na preparação de sujeitos pensantes, capazes de buscar continuamente novos caminhos. Estando assim, a universidades, além de ser ou dever ser uma instancia de produção de conhecimento, de cultura e de tecnologia, seria também a instituição em que pessoas, cidadãos e profissionais recebem a formação desejada. Tachizawa e Andrade (1999) corrobora esta ideia afirmando que “não há IES que sobreviva às exigências dos novos tempos se as expectativas de seus clientes não forem ouvidas”.

O contexto atual, com novas e renovadas demandas impostas às universidades, pressiona a busca de novas formas de atuação e de melhoria da qualidade dos serviços educacionais, desempenho e relevância dos serviços educacionais prestados. Meyer Jr (2014) reforçar que neste contexto, práticas são vistas como um processo dinâmico, complexo, interativo e social necessário para permitir as organizações universitárias integrarem esforços e agirem com estratégias adequadas respondendo aos desafios que se apresentam. Como veremos na próxima seção.

2.3. Segurança da Informação

Nesta seção, serão apresentados conceitos relativos à segurança da informação, bem como questões que demonstram a importância da elaboração, implementação e divulgação da Política de Segurança da Informação.

Conceitos e definições

> “Definições, assim como perguntas e metáforas, são instrumentos para fazer pensar. Sua autoridade reside inteiramente na sua utilidade, não na sua correção. Usamos definições a fim de delinear problemas que desejamos investigar, ou favorecer interesses que queremos promover. Em outras palavras, inventamos definições e as descartamos na medida em que servem aos nossos propósitos” (POSTMAN, 1980, p. 20).

É necessário conhecer inicialmente o conceito de informação para depois nos aprofundar no tema de SI. Segundo Campos (2007), a informação é um conjunto de dados que representa um ponto de vista. Um dado processado é o que gera uma informação, a partir do seu processamento, ele passa a ser considerado uma informação, que pode gerar conhecimento. Portanto, pode-se entender o conhecimento como uma reflexão da informação, e esta, por conseguinte o resultado do processo de significação dos dados (CAMPOS, 2007, p. 29). Para Davenport (1998), dados são imprescindíveis para a criação da informação, que por sua vez, faz parte do processo de construção do conhecimento permitindo que este seja consolidado. Lyra (2015) também traz de uma forma simples e direta, que a informação pode ser definida por um conjunto de dados tratados e organizados de tal maneira que tragam algum significado ou sentido dentro de um dado contexto. O que diferencia o uso da informação entre as organizações segundo Fontes (2012) é a necessidade de disponibilidade, a exigência de integridade e o rigor em relação ao sigilo que cada organização precisa para a sua informação.

Devido a grande importância da informação em nossa sociedade, a obrigação de protegê-la passou a ser crucial para as organizações. A ABNT (2005) normatiza que a informação precisa ser protegida adequadamente de maneira a garantir a sua confidencialidade, integridade e disponibilidade. Desta forma faz-se necessário definir também o conceito de Segurança da Informação.

A SI é definida por Sêmola (2014) como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”. Como diria Lyra (2008, p. 4), quando falamos em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente. A segurança da informação é um processo da organização e deve considerar a informação tanto no ambiente convencional quanto no ambiente de tecnologia, lembra Fontes (2012). E mesmo considerando que a maior parte das informações de uma organização esteja no ambiente de tecnologia, a utilização da informação acontece pelas pessoas, e estas estão no ambiente convencional. E a política? Uma política nada mais é do que um conjunto de regras que determina como deve ser o comportamento de pessoas que tem qualquer tipo de relacionamento com a organização no que diz respeito as informações que são trocadas, enviadas ou recebidas (CAMPOS, 2007).

Pilares de Segurança da Informação

Verificado os conceitos expostos acima, percebe-se um aspecto comum a todos eles: os elementos “confidencialidade, integridade e disponibilidade” tais elementos são os três pilares da segurança da informação.

Disponibilidade: “Garantia de que a informação e os seus ativos associados estejam disponíveis para os usuários legítimos de forma oportuna” (BEAL, 2008, p. 1). Ou seja, independente da finalidade, a informação deve estar disponível. A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (ABNT, 2005). O sistema deve estar disponível de forma que quando o usuário necessitar possa usar, define Reisswitz (2008).

Confidencialidade: “Garantia de que o acesso à informação é restrito aos seus usuários legítimos” (BEAL, 2008, p. 1). Ou seja, seu acesso é permitido apenas a determinados usuários. Confidencialidade é a propriedade de que a informação não esteja disponível a quem não tem autorização nem esteja credenciado (IN 01 GSIPR). A confidencialidade é apresentada sob o enfoque do sigilo, porém existe outro aspecto a considerar que é a ética de preservar ou guardar uma informação nem sempre classificada como sigilosa. Isto significa que nem sempre a informação tenha de receber um grau de sigilo para justificar a necessidade de medidas de proteção.

Integridade: A integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento (ABNT, 2005). “Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente”. (DANTAS, 2011, p11). “Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais” (SÊMOLA, 2014, p. 45). Ou seja, informação não adulterada.

Convém ressaltar que essas propriedades, apesar de isoladas, apenas tem valor se complementares. Por exemplo, não adianta uma informação estar disponível se a mesma não estiver integra.

Classificação da informação

A classificação da informação é fundamental para que as organizações possam direcionar os seus recursos para sistemas de segurança. Sabendo o nível de disponibilidade, confidencialidade e integridade das informações com quais a organização trabalha, esta pode gerar políticas de segurança da informação otimizadas e específicas para cada recurso. Para implementar uma boa política de segurança é necessário se conhecer a importância das diversas informações recebidas, utilizadas, armazenadas e transmitidas pela organização. Esta classificação da informação serve também para a organização conhecer melhor a o escopo, as rotas e necessidades de informação com que trabalha podendo fazer com que a informação tenha o fluxo necessário para o bom desenvolvimento dos seus trabalhos.

Todo o ciclo de vida da informação deve ser objeto da política. O manuseio ou uso da informação é a fase mais importante. É nessa etapa que os objetivos de integridade e disponibilidade tem destaque (BEAL, 2008). O armazenamento corresponde ao momento que a informação é guardada seja em um banco de dados, uma anotação em uma folha de papel, ou ainda, em um pendrive exposto na mesa de trabalho (SÊMOLA, 2014). Quanto mais capilar for a rede de transporte ou distribuição, mais eficiente será esta etapa. Fazendo chegar a informação certa a quem necessita dela para tomada de decisão (LYRA, 2008). Quando uma informação se torna obsoleta ou perde a utilidade para a organização, ela deve ser objeto de processo de descarte que obedeçam às normas legais, orienta Lyra (2015). Excluir

dos repositórios de informação corporativos os dados e as informações inúteis melhoram o processo de gestão da informação como economizando recurso de armazenamento, aumentando a rapidez e eficiência na localização da informação necessária dentre outros.

Portanto é estrutural que seja desenvolvida e implantada a política de segurança da informação para que todas as ações de proteção dos recursos de informação sejam bem direcionadas e adequadas à organização. A política definirá as diretrizes, os limites e o direcionamento que a instituição deseja para os controles que serão implantados na proteção de suas informações. A instituição terá referenciais para definição do escopo que delimita o campo de ação dos controles que serão desenvolvidos e implantados, fazendo com que o processo de SI possa ser avaliado adequadamente e somente terá resultado positivo se a sua implantação for uma decisão estratégica da organização e consequentemente a direção apoie explicitamente o desenvolvimento, a implantação e a manutenção de processo de proteção da informação, enfatiza Fontes (2012).

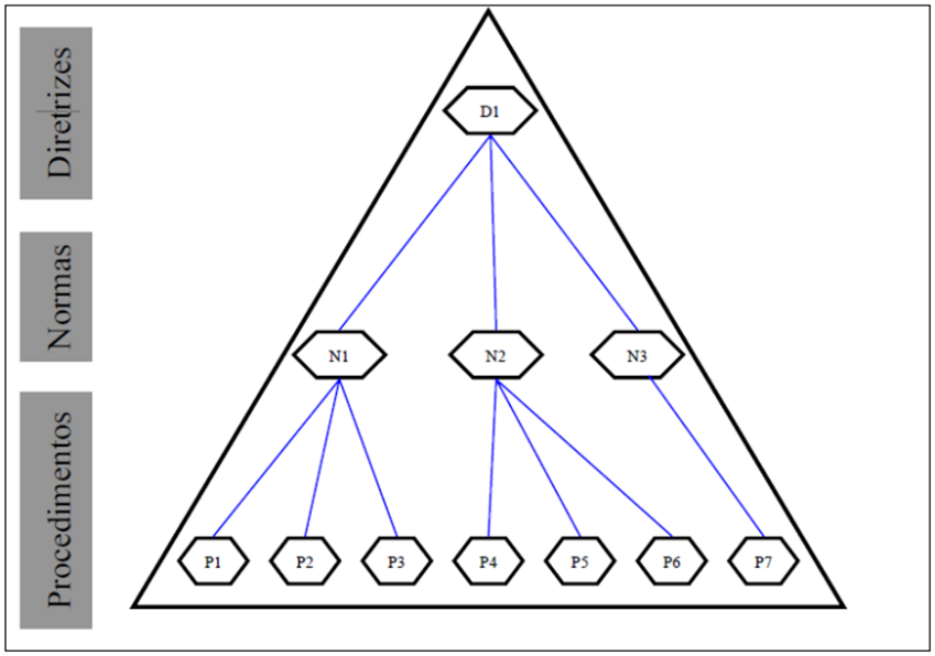
A melhor forma de evitar mal-uso das informações é educar seus usuários, assim é de vital importância que todo e qualquer usuário passe por uma formação antes de ter acesso às informações contidas no ambiente. Cada organização tem sua própria realidade e os níveis de segurança exigidos acabam sendo diferentes em cada uma (FONTES, 2006).

Política de Segurança da Informação

Para Castro (2002), a Política de Segurança da Informação é basicamente um manual de procedimentos que descreve como os recursos de que manipulam as informações da empresa devem ser protegidos e utilizados, e é o pilar da eficácia da Segurança da Informação, estabelecendo investimentos em recursos humanos e tecnológicos. Já Marciano e Lima-Marques (2006) detalham que uma política de segurança da informação é um conjunto de regras, normas e procedimentos que regulam como deve ser gerenciada e protegida a informação sensível, assim classificada pela organização ou pelo estado, além dos recursos e utilizadores que com ela interagem.

É apresentado, na figura 1, a relação de interdependência entre as estruturas normativas: diretrizes, normas e procedimentos, ou seja, se existir algum procedimento que não tem relacionamento com nenhuma norma, e alguma norma não tiver relacionamento com alguma diretriz, então a política de segurança estará incorreta. Há a necessidade de passar por uma revisão (CAMPOS, 2007).

Figura 1 – Visão conceitual da política de segurança.



Fonte: adaptado de Campos (2007).

A Diretriz (o que deve ser feito) é um documento elaborado pelo Comitê Gestor de Segurança da Informação (CSI) com base no planejamento estratégico corporativo e informacional descrito pela alta administração da organização (IMA, 2015). A partir dela é que são elaboradas e definidas as normas e procedimentos de Segurança da Informação.

A Norma (regras) é a especificação da forma e controle em que será feita a segurança da informação na organização de uma forma tática (IMA, 2015). Cada norma está associada a uma diretriz e aquela origina diversos procedimentos.

Já os Procedimentos (como fazer) são descrições passo a passo as atividades, responsáveis, evidências a serem produzidas, e ainda em um segundo momento, poderá ser adotado métricas que possibilitem a medida de eficiência e de nível de serviço auferido pelo processo (ABNT, 2005). Cada procedimento é documentado a partir de uma norma.

Adotar a implantação dos modelos através destes três níveis, possibilita a formalização dos processos recomendados pelas melhores práticas, e distribui o escopo de cada recomendação nos diversos níveis da organização.

O levantamento das questões, a recomendação dos controles e indicação dos riscos referentes à proteção da informação para organização é realizada pelo Gestor da Informação, sendo responsável pela gestão do processo de segurança da informação. Porém, é a direção e a área de negócio que devem definir o grau de rigor que devem ter os controles.

Diversos autores a exemplo de Sêmola e Fontes apoiam que os controles sugeridos pela ABNT ISSO /IEC 27002, são imprescindíveis e necessários para a construção de uma política de segurança da informação. A descrição completa dos controles deve ser consultada no texto integral da norma. Abaixo, segue os temas das 11 seções onde estão contidos os 133 controles que devem ser considerados e analisados se serão acatados pela política da organização.

1. Política de Segurança da Informação
   - Documento que deve conter os conceitos de segurança da informação, os objetivos e as formas de controle, o comprometimento da direção com a política, entre tantos outros fatores.
2. Organizando a Segurança da Informação
   - Estrutura para gerenciá-la; coordenada por representantes de diversas partes da organização; com responsabilidades definidas; e ter acordo de confidencialidade.
3. Gestão de Ativos
   - É qualquer coisa que tenha valor para a organização; deve ser identificado, classificado e seguir normas de utilização.
4. Segurança em Recursos Humanos
   - Antes da Contratação; Durante a Contratação; Encerramento ou mudança da Contratação.
5. Segurança Física e do Ambiente
   - De Equipamentos e instalações.
6. Gestão da Continuidade do Negócio
   - Visando impedir a interrupção das atividades do negócio e assegurar que as operações essenciais sejam rapidamente recuperadas.
7. Gestão de Operações e Comunicações
   - Gerenciamento de Serviços Terceirizados; Proteção contra Códigos Maliciosos e Códigos Móveis;
   - Cópias de Segurança; Gerenciamento de Segurança em Redes...
8. Controle de Acesso
   - Segurança dos Arquivos do Sistema, dos Processos de Desenvolvimento e de Suporte;
   - Controle de Acesso à Rede, ao SO, à aplicação e à informação...
9. Aquisição, Desenvolvimento e Manutenção de SI
   - Gestão de Vulnerabilidades Técnicas...
10. Gestão de Incidentes de SI
    - Procedimentos formais de registro e escalonamento devem ser estabelecidos
11. Conformidade
    - Conformidade com os Requisitos Legais; Conformidade com Normas e Políticas de SI e Técnicas...

3. METODOLOGIA

A Pesquisa tem natureza aplicada, pois depende de dados que podem ser coletados de diversas formas como ambientes do negócio, normas, padrões e procedimentos de segurança, plataformas computacionais. Explora problemas do mundo real como pesquisar uma estratégia de trabalho ou investigar qual abordagem de um tratamento, como exemplo a ausência de política de segurança da informação formalizada na instituição pesquisada. Esta aplicação prática e imediata dos resultados é o que distingue a pesquisa aplicada da pesquisa básica, que se concentra em questões teóricas. 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 a solução mais ou menos imediata do problema encontrado na realidade”.

A abordagem utilizada consiste em Estudo de Caso, uma metodologia qualitativa que visa aprofundar uma unidade individual a exemplo do campus I da Uneb. Conforme Yin (2015) o estudo de caso é uma estratégia de pesquisa que compreende um método que abrange tudo em abordagens especificas de coletas e análise de dados.

Será apresentado um conjunto de diretrizes que visam orientar, de acordo com os princípios da governança pública, a criação de novos sistemas de gestão de informação institucionais na Uneb. Tendo como objetivo transformar tais diretrizes em cláusulas imperativas e práticas, a constar no Regimento (BAHIA, 2012) da Universidade, pretendendo garantir que toda e qualquer ação voltada à criação de sistemas de gestão contribua, ao cabo, para a consolidação de uma gestão universitária transparente e, consequentemente, mais democrática.

Cabe a Uneb como entidade da Administração Pública do Poder Executivo Estadual, em conformidade com a Política de Segurança da Informação do Estado da Bahia, conforme o Artigo 3º do Decreto 13473/11:

- Gerir a SIC de forma permanente; de forma a garantir atualização e efetividade e continuidade do negócio.
- Mapear e avaliar periodicamente os processos de negócio quanto aos riscos da SIC; de forma a organizar e controlar os limites de riscos aceitáveis.
- Inventariar, classificar e proteger adequadamente os ativos de informação; definindo quais são os ativos, seus responsáveis, seus níveis de proteção, etc.
- Prover condições físicas e ambientais adequadas para o cumprimento das diretrizes da SIC; de forma a minimizar o acesso e a integridade dos ativos
- Elaborar e implementar programas de conscientização e capacitação em SIC de forma continuada; pois o usuário é o elo principal da corrente de segurança da informação.
- Complementar, quando for pertinente, as normas de Segurança da Informação necessárias à operacionalização desta Política. Permitindo flexibilidade e capacidade de expansão.

4. CONSIDERAÇÕES FINAIS

O presente projeto será desenvolvido em conjunto com a GERINF na elaboração dos Procedimentos de Segurança da Informação; fase de pesquisa sobre as melhores práticas em SI e formalização dos procedimentos para integração com as políticas institucionais existentes. Além disso, será proposta a criação de um CSI, composto por representantes de setores estratégicos da Uneb – para que seja desenvolvido o conteúdo das Políticas e Normas de Segurança; a definição propriamente da PSI, com atribuições e responsabilidades, classificação da informação, notificação e gerenciamento de incidentes. Além da aprovação e acompanhamento dos processos relacionados a SI. O esforço focado na mudança comportamental possibilitará maior probabilidade de obtenção de sucesso na segurança da informação.

REFERÊNCIAS

ABNT, NBR ISO/IEC 27.002: 2005 (antiga NBR ISO/IEC 17799: 2005) - Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2005.

ALAVI, Maryam; LEIDNER, Dorothy E. Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. MIS quarterly, p. 107-136, 2001.

BAHIA. Decreto 13.473 de 28 de novembro de 2011. Institui a Política de Segurança da Informação.

_____. Decreto 13.664 de 07.02.2012. Dispõe sobre o recredenciamento da Universidade do Estado da Bahia.

BARROS, Aidil J. da Silveira; LEHFELD, Neide A. de Souza. Fundamentos de metodologia, 2000.

BATTAGIN, I. L. da S., Norma não é lei. Mas por força da lei é obrigatória. Disponível em: <http://www.crea-sc.org.br/portal/index.php?cmd=artigos-detalhe&id=3077#.WDhRcFwRnr4> Acesso: agosto/20016.

BEAL, Adriana. Segurança da Informação. Princípios e melhores práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo: Editora Atlas – 2008.

CAMPOS, André – Sistema de Segurança da Informação: Controlando os Riscos. 2. ed. / André Campos. – Florianópolis: Visual Books, 2007.

_____, J. S; PRADO, R. C. A importância da conscientização sobre Segurança da Informação na Educação Infantil. Artigo, 2013.

CASTRO, Mauro. Política de Tecnologia da Informação no Brasil (Um guia para o século XXI). 1.ed.: Politec, 2002.

CHIAVENATO, Idalberto. Teoria geral da administração. Elsevier Brasil, 2002.

CRESPO, Marcelo Xavier de Freitas. O papel da educação digital e da segurança da informação no Direito. In: Âmbito Jurídico, Rio Grande, XIII, n. 79, ago 2010.

CROZATTI, Jaime. Modelo de gestão e cultura organizacional: conceitos e interações. Caderno de estudos, n. 18, p. 01-20, 1998.

DANTAS, Marcus Leal. Segurança da Informação: uma abordagem focada em gestão de riscos. Recife: Livro Rápido-Elógica, 2011.

DAVENPORT, Thomas H. Conhecimento empresarial. Elsevier Brasil, 1998.

FAVERO, M. De L. A universidade, espaço de pesquisa e criação do saber. Educação e filosofia, v. 13, n. 25, p. 249-259, 1999.

FONTES, Edison Luiz Gonçalves. Políticas e normas para a segurança da informação. Brasport, 2012.

_____, Edison Luiz Gonçalves. Segurança da Informação: o usuário faz a diferença. Saraiva, 2006.

GSIC. Gestão da Segurança da Informação e Comunicações: volume 1, UNB, 2010.

IMA. Informática de Municípios Associados S/A. Política de Segurança, disponível em: <http://www.ima.sp.gov.br/politica-de-seguranca-da-informacao> Acesso: 18 de março de 2017.

INSTRUÇÃO NORMATIVA GSI Nº 01, DE 13 DE JUNHO DE 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf> Acesso: 14 de nov. de 2016.

LYRA, Mauricio Rocha. (Org.) Governança da Segurança da Informação. 1º edição. Brasília, 2015.

_____, Maurício Rocha. Segurança e auditoria em sistemas de informação. Rio de Janeiro: Ciência Moderna, 2008.

MARCIANO, João Luiz; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. Ci. Inf., Brasília, v. 35, n. 3, p. 89-98, 2006.

MARÇULA, Marcelo; BENINI FILHO, Pio Armando. Informática: conceitos e aplicações. 2010.

MEYER JR, Victor. A prática da administração universitária: contribuições para a teoria. Revista Universidade em Debate, v. 2, n. 01, p. 12-26, 2014.

POSTMAN, Neil. Language education in a knowledge context. ETC: A Review of General Semantics, p. 25-37, 1980.

REISSWITZ, Flavia. Análise De Sistemas - Tecnologia Web & Redes. 2008.

SÊMOLA, Marcos. Gestão da segurança da informação. Elsevier Brasil, 2014.

SOUSA, Sofia Branco. A 'comunidade académica'como um conceito errático. Sociologia: Revista do Departamento de Sociologia da FLUP, XX, p. 149-166, 2010.

TACHIZAWA, Takeshy; DE ANDRADE, Rui Otávio Bernardes. Gestão de instituições de ensino. FGV Editora, 1999.

VALENTIM, Marta Lígia Pomim et al. O processo de inteligência competitiva em organizações. DataGramaZero, Rio de Janeiro, v. 4, n. 3, p. 1-23, 2003.

VARELA, Aida Varela. Informação, cognição e mediação: vertentes, contextos e pretextos. 2008.

YIN, Robert K. Estudo de Caso: Planejamento e Métodos. Bookman editora, 2015.