Segurança da informação e a Educação a distância

Hugo Toffalini Esteves dos Reis
hugotf@dcc.ufmg.br
Oficina de Lingua Portuguesa – Literatura e Produção de Texto

Resumo

Todos sabemos que qualquer software apresenta falhas e tais falhas poem em risco a segurança da informação alojada em tal software, podendo assim ser corrompida, alterada ou mal usada trazendo um mal para aqueles que dependem da mesma. Com a crescente utilização de softwares e da internet para as disciplinas de educação a distância uma indagação sobre a segurança da informação dentro de tais softwares e o impacto que todos os tipos de almeaças e vulnerabilidaes podem trazer ao estudantes, professores e universidades.

Palavras-chave: Educação a distância, segurança da informação

1 Introdução

Para trabalhar o tema, primeiro um conhecimento sobre a educação a distância teve que ser pesquisado, por isso é retratado conceitos sobre a educação a distância, o perfil dos alunos que nela estudam e as caracteristicas dos ambientes virtuais de aprendizagem, trazendo assim a educação a distância para o universo de problemas de segurança da informação que todo software apresenta. Uma explicação sobre segurança da informação então é feita, dando enfase a formas de vulnerabilidade, ameaças, ataques e mecanismos de segurança.

Toda esta exposição de conceitos é apenas para mostrar a base da pesquisa e para justificar as considerações que colocam de forma unica os problemas de segurança da informação e os softwares usados dentro da educação a distância.

2 Educação a distância

Segundo o Ministério da Educação e Cultura, educação a distância é uma “forma de ensino que possibilita auto-aprendizagem, com a mediação de recursos didáticos sistematicamente organizados, apresentados em diferentes suportes de informação, utilizados isoladamente ou combinados, e veiculados pelos diversos meios de comunicação”.

> Há um debate constante no mundo acadêmico sobre quem é levado a estudar on-line. Tem-se como fato dado que os alunos que estudam on-line são adultos, pois essa espécie de aprendizagem, que se dá em qualquer lugar e a qualquer hora, permite-lhes continuar trabalhando em turno integral sem deixar de também dar atenção à família. “O aluno on-line ‘típico’ é geralmente descrito como alguém que tem mais de 25 anos, está empregado, preocupado com o bem-estar da comunidade, com alguma educação superior em andamento, podendo ser tanto do sexo masculino quanto do feminino.” (GILBERT, 2001, p.74).

De acordo com Laaser, apud Mckenzie et al.(1979, p 17) o termo “educação a distância” adquiriu aceitação universal em 1982, quando o Conselho Internacional para a Educação por Correspondência (ICCE), uma organização afiliada à Unesco, mudou seu nome para Conselho Internacional para a Educação a Distância (ICDE). Segundo o Decreto nº. 5.622, de 19 de dezembro de 2005, caracteriza-se a educação a distância como modalidade

educacional na qual a mediação didáticopedagógica nos processos de ensino e aprendizagem ocorre com a utilização de meios e tecnologias de informação e comunicação, com estudantes e professores desenvolvendo atividades educativas em lugares ou tempos diversos. A educação a distância possui algumas vantagens em relação a outro tipo de ensino, pois a pessoa pode escolher tanto a hora de estudar quanto quando iniciar seus estudos. Como se sabe, cada aluno tem um ritmo de estudo próprio e a educação a distância permite que o aluno imponha seu ritmo individual e essa é uma grande vantagem da EAD. Possui, porém, algumas desvantagens tais como: os alunos podem sentirem-se isolados por estar realizando seus estudos sozinhos. Isso exige uma grande motivação por parte do aluno para continuar o curso desejado, visto que, caso contrário, possivelmente esse aluno desistirá deste curso. Esse é um dos maiores motivos da evasão no decorrer dos cursos a distância. Os meios telemáticos necessários ao ensino ainda não estão ao alcance de todos. A entidade formadora tem que disponibilizar um bom suporte para os alunos, além disso, o estudo pode se tornar muito teórico.

Analisando as características da educação a distância se percebe que elas se diferenciam muito do ensino presencial, pois podem até possuir o mesmo objetivo que é a transmissão de conhecimento, mas divergem bastante uma da outra na forma de se passar esse conhecimento. Enquanto o ensino presencial preocupa-se com o unitário, a EAD trabalha com o ensino em massa. Naquele, o professor está em sala de aula ajudando, mas controlando o aluno, neste o aluno faz seu horário de estudo, fazendo seu próprio controle.

3 O Aluno da educação a distância

Diferentemente do aluno do ensino presencial, que tem todo um ambiente ao alcance dele, o aluno que opta pela EAD possui algumas características próprias que são necessárias para estimular a percepção e a cognição do mesmo com a finalidade de prender sua atenção por longos períodos de estudo. A respeito desse assunto, o presidente da ABED (Associação Brasileira de Educação a Distância), Frederic Michael Litto em uma entrevista dada à folha on-line para a repórter Camila Marques em 2004 onde admitia que a modalidade "não é para todos". Pois segundo ele:

> O aluno que precisa do professor ao lado dele, cobrando ou elogiando, não é bom para ducação a distância. É preferível um aluno um pouco mais maduro, autônomo. E que cumpra os prazos.

Há algumas facilidades que pode ajudar esse aluno como a tecnologia usada, seja ela qual for, tem que ser bastante amigável e esse papel cabe ao professor que deve ter a capacidade de manter o interesse do aluno, motivando-o sempre.

3.1 Quem é o Estudante a Distância?

Estudos mostram que há uma preocupação constante em tornar a EAD cada vez mais centrada no aluno. De acordo com Belloni (2006 p. 39) “seja do ponto de vista dos aradigmas econômicos, seja desde a perspectiva das grandes definições” Para saber quem é o aluno da educação a distância é necessário analisar algumas características que lhes são peculiares. Segundo Belloni (2006):

> As características fundamentais da sociedade contemporânea que mais têm impacto na educação são, pois, maior complexidade, mais tecnologia, compressão das relações de espaço e tempo. Trabalho mais responsabilizado, mais precário, com maior mobilidade, exigindo um

> trabalhador multicompetente, multiqualificado, capaz de gerir situações de grupo, de se adaptar a situações novas, sempre pronto a aprender. Em suma, um trabalhador mais informado e autônomo.

Hoje em dia as pessoas procuram cada vez mais sua autonomia e a auto–aprendizagem é uma das características que mais se destacam no perfil dessas pessoas. O profissional atual precisa ser versátil e estar sempre ligado a novas tendências aprimorando seu aprendizado em prol do seu trabalho e até mesmo da sua realização pessoal. Trindade, apud Belloni (1992, p. 32), define aprendizagem autônoma como um processo de ensino e aprendizagem centrada no aprendente, e diz ainda que o professor deva assumir-se como recurso deste aprendente. Seria muito bom se esse fosse o perfil de todos os estudantes da educação a distância. Palloff e Pratt (2004), dizem que esse ideal de aluno está longe de fazer parte da grande maioria das pessoas que procuram esse tipo de ensino. De acordo com Renner (1995) muitos estudantes a distância tendem a realizar uma aprendizagem passiva "digerindo pacotes de informações e regurgitando os conhecimentos assimilados no momento de avaliação". Belloni (2006) diz que a clientela potencial da educação está se modificando rapidamente tendendo a aumentar em número e a se diversificar em termos de demandas especificas de globalização e localização. Gilbert, apud Palloff e Pratt (2004) diz que:

> O aluno on-line "típico" é geralmente descrito como alguém que tem mais de 25 anos, está empregado, preocupado com o bem-estar social da comunidade, com alguma educação superior em andamento, podendo ser tanto do sexo masculino quanto do feminino.

Pode se dizer que o aluno adulto da educação a distância atualmente encontra-se na fase da andragogia. Knowles (1995) define andragogia como "a arte e a ciência de ajudar adultos a aprenderem, partindo das diferenças básicas entre o Ser-adulto e o Ser-criança". Segundo este autor os adultos aprendem para uma aplicação imediata das atividades que executam, no sentido de resolver problemas.

Os jovens e as crianças aprendem com a finalidade de estocar conhecimentos. Considerando o público adulto, Knowles (1995), usando os princípios básicos da andragogia, entendendo também o modelo de curso adotado, e considerando as necessidades individuais de cada indivíduo cita os princípios desta ciência dizendo que eles permitem elaborar processos efetivos para a aprendizagem: necessidade de saber do estudante; autoconceito do estudante; experiência anterior do estudante; prontidão para aprender; orientação para aprender; motivação para aprender.

Pesquisas, porém, mostram que não há uma faixa etária definida para os cursos a distância. Palloff e Pratt (2004 p. 23) citam uma pesquisa publicada pelo *National Center for Education Statistics* (2002) que mostra que:

> Em 31 de dezembro de 1999, 65% das pessoas com menos de 18 anos haviam ingressado em um curso *on-line*, o que indica a popularidade crescente dos cursos virtuais de ensino médio. Cinqüenta e sete por cento dos alunos universitários considerados tradicionais, com idade entre 19 e 23 anos, também ingressaram em tais cursos. Cinqüenta e seis por cento das pessoas com idade entre 24 e 29 anos matricularam-se, e o índice de pessoas com mais de 30 anos que fizeram o mesmo foi de 63%. As estatísticas confirmam que o número de homens e mulheres e bastante semelhante. Com exceção dos grupos indígenas e dos nativos do Alaska (dos quais apenas 45% ingressaram em cursos on-line), cerca de 60% de pessoas de todas as raças participam de tais cursos.

Entende-se que o aumento da procura por cursos a distância se dá pelas facilidades que esse tipo de ensino pode oferecer. Com o uso da *Internet* houve uma facilitação maior visto que agora inexistem barreiras na comunicação entre o aluno e seu professor.

4 Ambientes virtuais de aprendizagem

O ambiente virtual de aprendizagem ou LMS (Learning Management System) é um software baseado na Internet que facilita a gestão de cursos no ambiente virtual. Existem diversos programas disponíveis no mercado de forma gratuíta ou não. O Blackboard é um exemplo de AVA pago e o Moodle é um sistema gratuito e de código aberto. Todo o conteudo, interação entre os alunos e professores são realizado dentro deste ambiente. De acordo com Clark e Mayer(2007), os ambientes virtuais são elementos fundamentais na tarefa de ensino, porém carecem de suporte pedagógico adequado em relação ao processo de aprendizagem.

4.1 O Ambiente Virtual de Aprendizagem: TELEDUC

Com o avanço da EAD, vários ambientes de aprendizagem virtuais foram criados cada um com características próprias, mas atuando sempre na mesma função, educar a distância.Serão mostradas algumas características do ambiente TelEduc. Rocha, apud Silva (2003 p. 377-378), diz que o TelEduc foi desenvolvido pelos pesquisadores do Núcleo de Informática Aplicada a Educação (NIED) da Universidade Estadual de Campinas (Unicamp) voltado para a formação de professores na área da informática na educação.

O ambiente TelEduc surgiu de uma proposta de mestrado, em 1997. Nessa época, de acordo com Freire e Prado apud Silva (2003), havia um conceito de formação centrada na construção contextualizada do conhecimento que era centrado no professor em sala de aula presencial durante todo o processo de formação do aluno. Como isso era inviável surgiu a idéia de criar esse ambiente virtual. Segundo Rocha (2003): “Trata-se de uma ferramenta que foi desenvolvida segundo pedido dos próprios usuários por isso é uma ferramenta participativa, de fácil acesso.” O ambiente TelEduc tem grande ênfase nas ferramentas de comunicação dando aos usuários a oportunidade de discutir, compartilhar e colaborar na elaboração de saberes. Os criadores dessa ferramenta de educação se preocuparam com a transparência e com a facilidade de uso. Por isso o ambiente possui uma *interface* bastante simples e amigável ao usuário. Seu primeiro uso foi no ano de 1998. Como a ferramenta foi aceita e se desenvolveu, disponibilizaram-na para uso em 2001, como *software* livre.

4.1.1 Características do ambiente virtual TELEDUC

O TELEDUC é dividido em:

- Ferramentas de coordenação: responsáveis por organizar as ações do curso.
- Ferramentas de administração: visão do formador do curso, responsáveis por apoiar o formador no curso.
- Ferramentas de comunicação: responsáveis pela interatividade entre os participantes do curso seja ele aluno ou professor.

5 Segurança da informação

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade CIA (Confidentiality, Integrity and Availability) -- Confidencialidade, Integridade e Disponibilidade -- representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a irretratabilidade e a autenticidade. Com o evoluir do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

Os atributos básicos (segundo os padrões internacionais) são os seguintes:

- *Confidencialidade* - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

- *Integridade* - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e destruição).

- *Disponibilidade* - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

O nível de segurança desejado, pode se consubstanciar em uma "política de segurança" que é seguida pela organização ou pessoa, para garantir que uma vez estabelecidos os princípios, aquele nível desejado seja perseguido e mantido.

Para a montagem desta política, deve-se levar em conta:

- Riscos associados à falta de segurança;
- Benefícios;
- Custos de implementação dos mecanismos.

5.1 Ameaças

Uma das definições apresentadas para ameaça é “evento ou atitude indesejável (roubo, incêndio, vírus, etc.) que potencialmente remove, desabilita, danifica ou destrói um recurso” (DIAS, 2000, p. 55). A mesma autora apresenta o item recurso como sendo “componente de um sistema computacional, podendo ser recurso físico, software, hardware ou informação” (DIAS, 2000, p. 55).

Com o advento das redes de longo alcance, principalmente a internet, tem-se uma característica complicadora para este cenário: a capacidade de anonimato, ou mesmo de desindividualização (ausência de características que permitam a identificação de autoria) das ações executadas em rede. Um usuário pode, em tese, se fazer passar por virtualmente qualquer outra pessoa, não importando de que etnia, gênero ou grupo social, desde que esteja disposto a tanto e tenha acesso aos recursos computacionais requeridos para esta tarefa, os quais são, em geral, são insuficientes. Tal situação é a tal ponto crítica que leva, em muitos casos, à adoção obrigatória de mecanismos de identidade eletrônica, como a certificação digital, à procura de modalidades seguras de autenticação de usuários.

Como exemplo de análise de ameaças à segurança da informação em ambientes computacionais, cite-se o estudo realizado em 2002 por Whitman (2003), o qual procurou responder a três questões primordiais:

1. quais são as ameaças à segurança da informação?
2. quais são as mais danosas ao ambiente organizacional?
3. qual a freqüência com que eventos baseados nelas são observados?

Em resposta à primeira pergunta, foram listadas doze categorias de ameaças potenciais, obtidas a partir de trabalhos anteriores e da entrevista com três security officers. Estas doze categorias são as seguintes, já dispostas em ordem decrescente de severidade percebida, conforme respostas obtidas pelo survey online realizado com organizações de diferentes portes e áreas de atuação (o autor não cita o número de instituições envolvidas na pesquisa):

1. eventos deliberados cometidos com o uso de software (vírus, vermes, macros, negações
de serviço);
2. erros ou falhas técnicas de software (falhas de codificação, bugs);
3. falhas ou erros humanos (acidentes, enganos dos empregados);
4. atos deliberados de espionagem ou invasão, hacking;
5. atos deliberados de sabotagem ou vandalismo (destruição de sistemas ou informação);
6. erros ou falhas técnicas de hardware (falhas de equipamentos);
7. atos deliberados de furto (de equipamentos ou de informação);
8. forças da natureza (terremotos, enchentes, relâmpagos, incêndios não intencionais);
9. comprometimento à propriedade intelectual (pirataria, infração a direitos autorais);
10. variação da qualidade de serviço (Quality of Service - QoS) por provedores (como energia elétrica e serviços de redes remotas de telecomunicação);
11. obsolescência técnica; e
12. atos deliberados de extorsão de informação (chantagem ou revelação indevida de informação).

Quanto à freqüência, os dados coletados por Whitman (2003) apontaram os resultados listados na Tabela 1.

5.2 Vulnerabilidades

Uma vulnerabilidade representa um ponto potencial de falha, ou seja, um elemento relacionado à informação que é passível de ser explorado por alguma ameaça - pode ser um servidor ou sistema computacional, uma instalação física ou, ainda, um usuário ou um gestor

de informações consideradas sensíveis. Dada a incerteza associada aos ativos e às vulnerabilidades

Número de eventos por mês	Nenhum	Até 50	De 51 a 100	Mais de 100	Sem Resposta
1. Eventos por software	16,7	62,5	9,4	11,5	
2. Erros ou falhas técnicas de software	30,2	64,6	5,2		
3. Falhas ou erros humanos	24,0	66,3	2,1	5,2	12,5
4. Espionagem ou invasão (*hacking*)	68,8	23,9	3,1	4,2	
5. Sabotagem ou vandalismo	64,6	34,4		1,0	
6. Erros ou falhas técnicas de hardware	34,4	62,5	3,1		
7. Furto	54,2	45,8			
8. Forças da natureza	62,5	36,5		1,0	
9. Comprometimento à propriedade intelectual	61,5	28,1	2,1	1,0	7,3
10. Variação de QoS	46,9	52,1	1,0		
11. Obsolescência técnica	60,4	37,5	1,0		1,0
12. Extorsão	90,6	9,3			

Tabela 1: Número mensal de eventos por ameaça, em percentual de respondentes (adaptada de Whitman (2003)).

a eles relacionadas, a construção de modelos probabilísticos tem sido utilizada para o mapeamento dos diferentes elementos da informação, na construção dos conjuntos de vulnerabilidades associadas a cada ativo. As diferentes soluções tecnológicas utilizadas na redução de vulnerabilidades sofrem de uma falha extremamente severa: estão em geral orientadas a vulnerabilidades específicas e sua utilização, potencialmente, pode introduzir novas vulnerabilidades. Diversas soluções têm sido tentadas, como a aplicação de algoritmos genéticos para a criação de perfis de segurança voltados a situações genéricas (GUPTA et al., 2004), mas um longo caminho ainda está por ser percorrido. Também o prognóstico de vulnerabilidades, ou seja, a tentativa de identificar áreas ou servidores computacionais em uma rede que podem se mostrar vulneráveis em um momento futuro, com o uso de recursos como lógica nebulosa (VENTER; ELOFF, 2004), carece de maiores desenvolvimentos.

Há que se observar que estas e outras propostas, dependentes de recursos tecnológicos como são, podem se ver, por si mesmas, sujeitas a vulnerabilidades, realimentando o ciclo de procura por soluções efetivas ao problema. De fato, o relatório IT Governance Institute (2004c) indica que grande parte dos gestores enxergam a importância da Tecnologia da Informação - TI para atingir a estratégia da organização, mas 41% dos respondentes a este survey vêem como problema uma visão inacurada da performance da tecnologia da informação - ou seja, não têm um panorama claro do andamento do setor de informação em suas próprias organizações.

5.3 Incidentes

O Internet Engineering Task Force - IETF, organização independente dedicada à análise e prevenção de eventos de segurança e à gestão da rede, define incidente como sendo "um evento que envolve uma violação de segurança" (SHIREY, 2000). Uma definição mais voltada à autoria e ao tipo do evento é dada por Howard e Meunier (2002): "um ataque ou um grupo de ataques que pode ser diferenciado de outros ataques pela distinção dos atacantes, ataques, bjetivos, sites e ocasião".

5.4 Ataques

Por sua vez, um ataque corresponde à concretização de uma ameaça, não necessariamente bem-sucedida (do ponto de vista do atacante), mediante uma ação deliberada e por vezes meticulosamente planejada. Uma vez que a geração de ataques é originada por pessoas, ainda que com o uso de recursos computacionais ou de outra natureza, a sua prevenção torna-se extremamente complexa por meios automatizados. De fato, Schell (2001)

afirma que não há ciência capaz de eliminar definitivamente os incidentes de segurança da informação, restando a opção da constante vigilância e verificação. Deve-se observar, ainda, que os ataques podem ser de origem externa ou interna à organização. Schultz (2002) aponta que os ataques de origem interna, que, ao contrário do que se apregoa, não necessariamente são em maior número que os externos, possuem motivações e padrões diversos daqueles, exigindo, assim, análise e contramedidas diferenciadas.

5.5 Mecanismos de segurança

O suporte para as recomendações de segurança pode ser encontrado em:

- *Controles físicos*: são barreiras que limitam o contato ou acesso direto a informação ou a infra-estrutura (que garante a existência da informação) que a suporta.
  Existem mecanismos de segurança que apóiam os controles físicos:

  Portas, trancas, paredes, blindagem e guardas.

- *Controles lógicos*: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.
  Existem mecanismos de segurança que apóiam os controles lógicos:

  - *Mecanismos de criptografia*. Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.
  - *Assinatura digital*. Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade.
  - *Mecanismos de garantia da integridade da informação*. Usando funções de "Hashing" ou de checagem, consistindo na adição.
  - *Mecanismos de controle de acesso*. Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
  - *Mecanismos de certificação*. Atesta a validade de um documento.
  - *Integridade*. Medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos.
  - *Honeypot*: É o nome dado a um software, cuja função é detectar ou de impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.
  - *Protocolos seguros*: uso de protocolos que garantem um grau de segurança e usam alguns dos mecanismos citados aqui.

Existe hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os anti-vírus, firewalls, firewalls locais, filtros anti-spam, fuzzers e analisadores de código.

6 Considerações Finais

6.1 Segurança da informação e a EAD

Ao falar sobre o conceito de educação a distancia se caminha lado a lado com a internet e sistemas computacionais que necessitam ser cada vez mais interativos e proporcionar as melhores ferramentas para a evolução do aprendizado dos estudantes. Como aqui exposto, todo sistema apresenta seu problemas quanto a segurança da informação e por que o sistemas de EAD ficariam de fora? Pois não ficam, basta utiliza-los que ja encontramos falhas como as descritas por Whitman(2003), porem EAD trata de um conjunto de deveres e informações muito valiozos e que precisam ser cuidados de forma mais mais adequada.

Atualmente não pode-se garantir quem esta do outro lado do computador concluindo as atividades, não podemos garantir que a prova ou os trabalhos entregues não estao sendo copiados por outras instituições e como aqui mesmo foi sitado, o perfil dos alunos de EAD é vasto e nem sempre todos os alunos tem a maturidade para serem honestos com o processo e utilizam das falhas do sistema para garantirem certificados, diplomas, créditos de forma mais facil. Tais falhas somadas com problemas em conclusão dos modulos dos cursos devido a falhas de hardware, software ou até mesmo humanas denigrem a imgem de um curso ou até mesmo de uma instituição.

Providências tem que ser tomadas para tornar a informação dentro da EAD algo mais confiavel e por isso mecanismos de segurança como aqui sitados devem ser adotados, como biometria para o acesso ao sistema garantindo a indentidade do usuário, sistemas blindados a copia com alta nivel de criptografia, principalmente nas produções dos alunos e uma infra-estrutura de hardware robusta e com profissionais capacitados para manter as ferramentas sempre operacionais para que o aluno não sofra com nenhuma restrição de horário.

Referências

BELLONI, Maria Luiza. **Educação a Distância**. 4.ed.São Paulo: Autores associados, 2003.

CLARK, Ruth Colvin; MAYER, Richard E. ***e-Learning and the Science of Instruction: Proven Guidelines for Consumers*****:** and Designers of Multimedia Learning. New York: Pfeiffer, 2007. pp. 496

DIAS, C. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel, 2000.

GUPTA, M. et al**. Matching information security vulnerabilities to organizational security profiles**: a genetic algorithm approach. Decision Support Systems, 2004.

HOWARD, J. D.; MEUNIER, P. **Using a "common language" for computer security incident information.** In: BOSWORTH, S.; KABAY, M. E. (Eds.). Computer Security Handbook. 4th. ed. New York: John Wiley & Sons, 2002. p. 3.1–3.22.

KNOWLES, M. (1975). **Self-Directed Learning**. Chicago: Follet. LAASER, Wolfram et al. **Handbook for designing and writing distance education materials**. copyright, 1989.

MEC, **Regulamentação da EAD no Brasil**, disponível em http://portal.mec.gov.br/default.htm acesso em 4 de novembro de 2011.

MENDONÇA, Alzino Furtado de et al. **Metodologia Científica**: guia para elaboração e apresentação de trabalhos acadêmicos. Goiânia: Faculdades Alves Faria, 2003.

NIED , **TelEduc,** disponível em< http://teleduc.nied.unicamp.br/> acesso em 6 de novembro de 2010.

PALLOFF, Rena M; PRATT, Keith. **O Aluno Virtual**: um guia para trabalhar com estudantes on-line. Porto Alegre: Artmed, 2004.

ROPOLI, Edilene. **Orientação para desenvolvimento de cursos mediados por computador.** Maio 2004.

SCHELL, R. R. **Information security**: science, pseudoscience and flying pigs. In: 17th **Computer Security Applications Conference**. [S.l.]: ACSAC, 2001. p. 205–216.

SHIREY, R. RFC 2828 - Internet Security Glossary. 2000. Disponível em:< http://www.ietf.org/rfc/rfc2828.txt >. Acesso em: 1 de novembro de 2010

SCHULTZ, E. E. **A framework for understanding and predicting insider attacks**. Computers & Security, v. 21, n. 6, p. 526–531, Oct. 2002.

VENTER, H. S.; ELOFF, J. H. P. **Vulnerability forecasting: a conceptual model**. Computers & Security, v. 23, n. 6, p. 489–497, Sept. 2004.

WHITMAN, M. **E. Enemy at the gate: threats to information security**. Communications of the ACM, v. 46, n. 8, p. 91–95, Aug. 2003.