Análise da segurança de informação nos contextos de *cloud computing*.
Estudo exploratório realizado junto de utilizadores universitários portugueses.
Galvão Meirinhos

Abstract
The recent emergence of cloud computing is directly related to the infrastructure architecture that allows ubiquitous, elastic and versatile computing. This innovative architecture has once again raised the issue of information and communications security. The transition to the client/server model has opened up new challenges and uncataloged risks, where traditional security systems of on-premises information systems are unable to develop the feeling and perception of security in the contexts of cloud computing. The efficiency and effectiveness of traditional security mechanisms are being questioned, generating distrust and fears in many cloud computing users.

Keywords
Information security, cloud computing, cloud services.

Na sociedade ocidental a interação social e empresarial é progressivamente mediatizada por computadores, que assumem um papel central na instalação do conceito da sociedade da informação e da comunicação. Este sistemas são cada vez mais ameaçados pelas dimensões técnicas e humanas do fenómeno da insegurança informática, que colocam a existência singular e colectiva em causa, representando sempre prejuízos e perdas dificilmente determináveis. A sociedade de informação é um projeto que marca e abrange todos os sujeitos que conformam o colectivo humano. A interconexão entre sistemas de informação é um meio de promoção das comunicações e da partilha de informações de toda e qualquer ordem, cuja partilha conforma um real perigo tanto para a segurança individual dos cidadãos (Araújo 2005:5), como para a segurança económico-financeira das organizações.

A lógica recente da partilha de recursos e aplicações *on-demand* sem esforço de gestão (Mell, Peter; Grance, Timothy; NIST, 2011) acarreta todo um novo cenário de insegurança e preocupação coletiva. Por causa deste facto, o armazenamento de dados e informações nessas plataformas pode afetar decisivamente a existência e o desenvolvimento das organizações. Por isso, e com o interesse do estudo desta problemática em contexto real, pensamos estudar o assunto no contexto universitário, porque intuímos que a partilha de informação entre os jovens e estudantes universitários nos *cloud services* segue o mesmo padrão de partilha descuidada e sem noção das consequências pessoais.

A resposta silenciosa passa pela cultura de segurança que compreende o comportamento experiente, a participação contínua e a verificação constante da realidade por parte de pessoas e organizações. Estas práticas conscientes são a única forma de combater as ameaças físicas e virtuais que afetam pessoas e organizações. Deste forma, o problema de conhecimento deste trabalho é: Será que o estudante universitário confia na segurança da informação armazenada na *cloud*? Com base nesta pergunta de investigação, os objectivos são: analisar a problemática dos comportamentos individuais em torno da partilha e segurança de dados e informações nos *cloud services*; equacionar a confiança dos utilizadores nos *cloud services*; e, estimar um índice de segurança de informação dos diferentes *cloud services* na óptica dos alunos universitários.

A metodologia do presente trabalho científico é de natureza exploratória. O estudo empírico foi realizado em contexto universitário, entre outubro e dezembro de 2016, junto de uma amostra de 284 sujeitos maiores de idade, que responderam de livre vontade e sem qualquer reserva de participação. Os questionários foram aplicados em distintos ciclos de estudos (licenciatura, mestrado e doutoramento) da Universidade de Trás-os-Montes e Alto Douro, por forma a incrementar significativamente a perspetiva radiográfica do fenómeno da cultura de segurança da informação nos *cloud services*. No plano dos resultados, verificamos variações significativas na confiança nos *cloud services* segundo o género, a faixa etária e formação académica, embora os comportamentos individuais de partilha de dados sejam muito similares.

A recente emergência do *cloud computing* está diretamente relacionada com a arquitetura da infraestrutura que permite a computação ubíqua, elástica e versátil. Esta arquitetura inovadora lançou de novo a problemática da segurança da informação e das comunicações. A transição para o modelo cliente/servidor abriu novos desafios e riscos não catalogados, onde os sistemas tradicionais de segurança dos sistemas de informação locais são incapazes de desenvolver a sensação e a percepção de segurança nos contextos do

cloud computing. A eficiência e eficácia dos mecanismos tradicionais de segurança estão a ser colocados em causa, gerando desconfianças e temores em muitos utilizadores do *cloud computing*.

A arquitetura do *cloud computing* assenta no acesso a recursos tecnológicos externos, nomeadamente no acesso *on-demand* de aplicações empresariais e de armazenamento. Neste contexto, o utilizador pode configurar uma série de recursos de computação, tais como servidores, redes, sistemas de armazenamento, aplicações e serviços. Todas estas configurações podem ser realizadas sem qualquer esforço de gestão mediante interações simples e inteligíveis. No plano físico, processadores, discos duros e dispositivos de rede estão algures nos denominados *datacenters*, que assumem a função de processamento e armazenamento. As utilidades do *cloud computing* advêm da tecnologia de virtualização, passando a ser um fator crítico das implementações independentes, económicas, escaláveis, partilhadas, rápidas e flexíveis.

A expressão *cloud services* absorve uma série de significados que vão desde da distribuição de aplicações e serviços até à implementação e gestão de vários recursos e dispositivos cuja propriedade por ser privada, pública ou comunitária. Neste âmbito, existem basicamente três modelos de serviço, nomeadamente a infraestrutura como serviço (IaaS), a plataforma como serviço (PaaS) e o *software* como serviço (SaaS). Na IaaS, a infraestrutura remota oferece uma série de capacidades na área do processamento, armazenamento e redes, bem como o controlo do sistema operativo e aplicações. Na PaaS, a plataforma remota oferece um conjunto de possibilidades de instalação de sistemas operativos e aplicações adquiridas ou desenvolvidas através de aplicações de desenvolvimento fornecidas pelo fornecedor do *cloud service*. E, por fim, o SaaS consiste num modelo de distribuição de software instalado numa infraestrutura ou plataforma baseada na tecnologia do *cloud computing*. As aplicações são acessíveis a partir de uma grande variedade de dispositivos fixos ou móveis, cuja utilização pode ser remunerada ou gratuita.

Os riscos e as ameaças à segurança da informação não conhecem fronteiras, sendo cada vez mais uma preocupação global dos órgãos públicos, das empresas e dos cidadãos. O aumento contínuo dos riscos e ameaças tem levado à promoção de políticas de segurança física e lógica da informação digital, que passam pela formação de pessoas, equipamentos, instalações, gestão de acessos e contramedidas. A segurança da informação versa sobre a proteção de um conjunto de dados e informações com valor sob qualquer formato e suporte, por forma a preservar a sua integridade, disponibilidade, confidencialidade e autenticidade (Beal 2005:71). A proteção implica sempre conhecer bem as ameaças e as vulnerabilidades físicas, tecnológicas e humanas. Relativamente à última vulnerabilidade, Eduardo Araújo afirma que (...) o fator humano é o principal desafio para se ter uma boa e segura conduta de segurança da informação (Araújo 2005:5). A segurança é, antes de mais, conhecimento, atitude e comportamento que, quando devidamente orientados, resolvem grande parte dos problemas que decorrem da (in)segurança da informação. A resposta silenciosa passa pela cultura de segurança que compreende o comportamento experiente, a participação contínua e a verificação constante da realidade por parte de pessoas e organizações. Estas práticas conscientes são a única forma de combater as ameaças físicas e virtuais que afetam pessoas e organizações.

Um dos maiores desafios contemporâneos é saber se o sujeito consegue gerir a confidencialidade dos seus dados pessoais e a privacidade das suas relações eletrónicas. No mundo atual, a privacidade dos dados pessoais passou a ser uma realidade abstrata porque, no plano jurídico, não é evidente a fronteira do que é informação pessoal e informação pública, onde múltiplos agentes exploram a opacidade do tema, quase nunca sem o conhecimento completo e prévio do cidadão. Por outro lado, concorrem os aspetos da cultura da segurança da informação frequentemente negligenciados, e episodicamente postos em causa por perguntas tão simples como: "*Autoriza a divulgação dos dados fornecidos para futuras ofertas comerciais?".* Quando ocorrem situações destas, estamos perante a solicitação do consentimento expresso. Porém, e em muitas outras situações, quando concordamos com a situação A despoletamos uma situação B, que conforma um consentimento tácito ao tratamento e à divulgação dos dados pessoais. A existência do consentimento tácito é a porta aberta ao atropelo dos direitos dos cidadãos, especialmente no que toca à confidencialidade da informação e à privacidade do cidadão. A maior parte dos sistemas de informação, com que lidamos diariamente, são-nos apresentados como instrumentos de valor acrescentado para o nosso conforto e produtividade, sempre com apelativas chamadas para a redução de custos. Ainda assim, a cultura de segurança e o comportamento preventivo do cidadão perante a gestão da informação, são o garante dos seus direitos e liberdades numa sociedade cada vez mais competitiva, conflituosa e ávida de conhecimento dos seus interlocutores. A partilha de informações do foro pessoal deverá ser sempre feita de livre vontade e de

forma totalmente esclarecida, permitindo ter a noção das repercussões futuras dos nossos consentimentos e adesões.

Segundo o IT Governance Institute, a gestão da segurança da informação é responsabilidade de todos os membros e utilizadores quanto à aplicação de normas e procedimentos de segurança (ITGI, 2006:11). A responsabilização progressiva dos intervenientes é a raiz do desenvolvimento da cultura de segurança da informação, onde o risco é minimizado pelo nível de sensibilização das pessoas, contribuindo, desta forma, para a melhoria da segurança dos sistemas de informação e das redes de dados. As grandes empresas levam estes assuntos da segurança da informação muito a sério, dado que planeiam, implementam e avaliam o cumprimento das disposições internacionais sob a forma de normas e procedimentos. Por outro lado, a segurança dos sistemas e redes de informação deve respeitar os valores das sociedades democráticas, a livre circulação da informação, bem como os princípios de respeito pela vida privada do cidadão. Com base nos valores e na ética, a Organização para a Cooperação e Desenvolvimento Económico (OCDE, 2002:17-23) apresenta nove princípios base para alicerçar uma cultura de segurança da informação:

- Sensibilização – todos os intervenientes devem ser conhecedores dos riscos, no sentido de serem a primeira linha de defesa para a segurança da informação;
- Responsabilidade – todos os participantes são responsáveis pela segurança dos sistemas e redes de informação;
- Reação – todas as pessoas devem agir com prontidão e numa atitute mental dominante baseada na cooperação na prevenção, deteção e resposta aos incidentes de segurança;
- Ética – todo e cada participante deve respeitar os legítimos interesses das partes interessadas. O comportamento ético é indispensável para evitar danos e prejuízos por ação ou inação;
- Democracia – a segurança dos sistemas de informação deve respeitar os princípios das sociedades democráticas, como a liberdade, igualdade e fraternidade;
- Avaliação do risco – os sistemas e redes de informação devem ser alvo, periodicamente, de avaliações de vulnerabilidades, para determinar o nível aceitável de risco e selecionar as medidas de combate às ameaças;
- Conceção e delineamento da segurança – os níveis de segurança desejados definem a arquitetura dos sistemas e redes de informação. As medidas de proteção da informação envolvem soluções lógicas e físicas;
- Gestão da segurança – a segurança assenta na cobertura e na avaliação de todas as atividades das partes interessadas mediante procedimentos para a resolução dos incidentes;
- Reavaliação – as vulnerabilidades e as ameaças são crescentes e evolutivas, o que pressupõe que as partes interessadas tenham de rever continuamente as políticas, os procedimentos e as medidas de segurança.

São cada vez mais as empresas que seguem estes princípios da cultura de segurança da informação, uma vez que as perdas podem ser substanciais, inclusivamente podem mesmo levar à falência e extinção da própria organização. A instalação definitiva da cultura de segurança da informação no plano pessoal e empresarial é uma questão de tempo, porque vivemos num mundo cada vez mais ubíquo, conflituoso e inseguro. Vejamos o caso da segurança dos dados pessoais que deveriam ser protegidos pelas autoridades públicas nacionais. Em Portugal, existe um Gabinete Nacional de Segurança com independência administrativa, mas na dependência direta do Primeiro-Ministro ou de outro membro do Governo ao qual o Primeiro-Ministro tenha delegado competência para tal. Esta entidade é dirigida pela Autoridade Nacional de Segurança, cuja função é exercida e se destina a proteger, de forma exclusiva, a informação previamente classificada. É aqui que reside precisamente o problema: o Estado tem alguma dificuldade em proteger os dados do cidadão comum.
Havendo a consciência de que a segurança dos dados pessoais se caracteriza por ser um tesouro cuja posse pertence apenas ao indivíduo, faz com que seja exigida a sua preservação e confidencialidade no âmbito do direito intransmissível desses mesmos dados, desde que não exista a prévia autorização do fornecimento dos mesmos. A preocupação e reserva de alguns cidadãos em não fornecer informações de caráter pessoal é legítima e é uma excelente opção, que deve ser respeitada, e em caso algum, violada. A recolha de informação pessoal coloca em risco a segurança individual e começa a percecionar-se como uma séria ameaça. A fim de colmatar este desígnio, vemos, com alguma pertinência, a necessidade de ser criado um sistema de codificação com simbologia própria, cujos dados passariam a ser registados, minimizando o grau de risco do crime da sua divulgação. Torna-se, assim, uma necessidade imperiosa a aplicação desta metodologia, de modo a garantir a confidencialidade da informação.

Atualmente, os padrões dos sistemas de segurança da informação estão definidos numa série de normas. A ISO 27000 contém as definições utilizadas em toda a série de normas 27000. A aplicação do padrão necessita de um vocabulário claro e sem ambiguidades, por forma a evitar significados distintos para os mesmos conceitos técnicos e de gestão, presentes em todos os documentos da série. A norma ISO 27001 é a principal norma que apresenta todos os requisitos de um sistema de segurança da informação de gestão. Dentro da série de normas ISO 27000, temos também a norma 27002 (código de práticas), a 27003 (guia de implementação), a 27004 (métricas e medição), a 27005 (gestão do risco) e a 27006 (diretrizes de serviços de recuperação de desastres). Este normativo configura o padrão da certificação dos sistemas de informação baseados em políticas de segurança, de controlo e de gestão de riscos. No caso concreto da norma ISO 27001, define os requisitos para o estabelecimento, a implementação, a operacionalização, a monitorização, a revisão, a manutenção e a melhoria da gestão de segurança da informação. Assim sendo, o documento, que foi publicado em outubro de 2005, pretende:

- Estabelecer uma metodologia para as questões da gestão da segurança;
- Reduzir o risco de incidências como a perda, roubo ou adulteração da informação;
- implementar medidas de segurança relativas ao acesso à informação;
- Definir regras de comportamento para todos os interessados da organização;
- Gerir processos subjacentes ao princípio da segurança planeada e em condições controladas;
- Conformar a gestão da segurança com a legislação sobre informação pessoal, propriedade intelectual e outras;
- Avaliar os riscos e as ameaças continuamente.
  Todas as considerações lavradas nas normas da série ISO/EIC 27000 são universais e adaptáveis a todos os tipos de organizações comerciais, públicas, associativas, entre outras. Neste contexto, os padrões internacionais de segurança da informação assentam na:
- Confidencialidade – propriedade que condiciona o acesso às entidades e/ou pessoas autorizadas pelo proprietário da informação;
- Integridade – propriedade que garante que a informação manté mas características originais, incluindo o controle das alterações e garantia do ciclo de vida da informação;
- Disponibilidade – propriedade que garante que a informação esteja sempre disponível aos utilizadores autorizados pelo proprietário da informação;
- Autenticidade – propriedade que garante que a informação é originária, não tendo sofrido subtrações ou adições de dados;
- Irretratibilidade – propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anterior.

Associados a estes atributos principais estão os mecanismos de segurança física e lógica. Os mecanismos físicos passam por barreiras que limitam o contacto ou o acesso direto à informação, como a existência de portas, trancas, paredes especiais, blindagens, segurança com presença humana, entre outros. Os controlos lógicos são barreiras eletrónicas e digitais que impedem ou limitam o acesso à informação. Ainda no âmbito dos controlos lógicos, os mecanismos de segurança podem ser baseados na encriptação (transformação reversível da informação por forma a ser ininteligível a terceiros); na assinatura digital (dados criptográficos relacionados com um documento que garanta a sua integridade e autenticidade, embora a sua confidencialidade possa ser posta em causa); no *Hashing* (verificação comparativa entre a informação local e a informação disponibilizada pelo autor/proprietário) e controlos de acesso (baseados em senhas, dados biométricos, cartões inteligentes, etc.). O território dos mecanismos é sempre um cenário em aberto, aparecendo progressivamente outros mecanismos cada vez mais sofisticados e resistentes às ameaças informáticas.

METODOLOGIA

A metodologia do presente trabalho científico é de natureza exploratória. O estudo foi realizado em contexto universitário junto de uma amostra de 284 sujeitos maiores de idade, que responderam de livre vontade e sem qualquer reserva de participação. Os questionários foram aplicados em distintos ciclos de estudos (licenciatura, mestrado e doutoramento), por forma a incrementar significativamente a perspetiva radiográfica do fenómeno da cultura de segurança da informação nos *cloud services*. A exploração teórico-prática permitiu desenvolver uma visão geral do fenómeno da segurança da informação nos contextos tradicionais e nos novos contextos de computação em regime de *outsourcing*. É nossa convicção que este trabalho pode constituir uma

boa base para outros consequentes, porque constatámos uma reduzida produção científica sobre a percepção e confiança dos utilizadores nos contextos do *cloud computing*.

QUESTIONARIO

Neste trabalho de investigação, utilizámos um questionário estruturado, misto e auto-administrado, formado por seis questões, das quais quatro são de modalidade de resposta fechada de escolha múltipla, e duas de modalidade de resposta fechada dicotómica. No âmbito das escalas, foram usadas escalas de resposta psicométrica do tipo *Likert* em quatro questões fechadas de escolha múltipla. Quanto à estrutura do questionário, consideramos quatro questões sobre o conhecimento e riscos individuais de uma série de situações concretas, uma relacionada com os mecanismos de proteção e preservação da informação e, uma última, sobre o conhecimento do nível de segurança nos *cloud services* usados pelos alunos. Foi também recolhida informação relacionada com a idade, género, idade e o ciclo de estudos que frequenta na Universidade de Trás-os-Montes e Alto Douro. Por outro lado, a ordem das questões no seio da estrutura foi ponderada por forma a evitar qualquer contaminação ou indução das respostas entre questões. Como medida de consistência interna, o questionário apresenta um alfa de cronbach de 0.852, o que revela um grau de confiabilidade do questionário importante.

TRATAMENTO DE DADOS E DISCUSSÃO DOS RESULTADOS

A codificação e a tabulação dos dados foi levada a cabo com a aplicação de tratamento de dados SPSS Statistics, onde temos 10 variáveis com escalas nominais, 20 com escalas métricas de intervalo e uma com escala métrica de razão, totalizando 31 variáveis tipificadas com três tipos de escalas. A introdução dos dados foi feita de forma organizada e cuidada para termos a completa noção das sub-amostras relacionadas com os diferentes ciclos de estudos. Este procedimento permite-nos fazer análises globais dos dados, bem como uma série de análises parcelares ou sub-amostrais, com o intuito de perceber as diferenças entre contextos formativos. A análise estatística dos dados foi iniciada pela geração das tabelas de frequências absolutas e relativas e tabelas cruzadas. No sentido de apurar correlações entre as diferentes variáveis foi calculado o coeficiente de correlação de Pearson.

De seguida, apresentamos os resultados obtidos que se conformam como as respostas às nossas perguntas de investigação. Entre outubro e dezembro de 2016, participaram no estudo 284 alunos com idades compreendidas entre 18 e 55 anos. A amostra era constituída por 193 alunos de licenciatura, 65 alunos de mestrado e 26 alunos de doutoramento, dos quais 96 eram do género masculino e 188 do género feminino. As idades compreendidas no intervalo de 19 a 21 anos representam cerca de 68.3% do total dos alunos que responderam ou participaram na investigação.

Em relação à primeira questão, 252 dos 284 alunos escolheram a resposta correta sobre o significado de segurança de informação[1], representando 88.7% do total dos inquiridos. No âmbito da análise das sub-amostras, verificamos que a resposta correta foi dada por 172 dos 193 alunos de licenciatura, 55 dos 65 alunos de mestrado e 25 dos 26 alunos de doutoramento. Constatamos que existe um conhecimento generalizado do que significa a segurança de informação.

Em relação à segunda questão, e no âmbito dos níveis de risco, os inquiridos consideram que: dar a conhecer senhas de acesso (M=2.52); não ter antivírus atualizados (M=2.97); instalar software de origem desconhecida ou duvidosa (M=2.97); abrir ficheiros que vem anexados aos emails (M=2.88); abrir programas e ficheiros presentes em CD que acompanham as publicações periódicas ou livros (M=2.33); utilizar aplicações de mensagens instantâneas (M=2.78); e, inserir informações pessoais em formulários electrónicos (M=2.93), apresentam riscos compreendidos entre o nível baixo e o nível de risco relativo. Não obstante, verificamos que as realidades da partilha de pens drives, CD e DVD entre amigos e colegas de trabalho (M=3.13); navegar na World Wide Web (M=3.1) e as práticas de download/upload de programas e ficheiros (M=3.2), apresentam, na óptica dos inquiridos, um nível de risco relativo. Ou seja, as dez situações inventariadas apresentaram, como valor minion, uma média de 2.1 e como, valor máximo de 3.2, o que quer dizer que as situações de instalação, utilização, partilha, navegação são consideradas práticas de baixo risco ou riscos relativos.

[1] A segurança da informação consiste em proteger um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

Quanto à terceira questão, relacionada com o conhecimento dos mecanismos de proteção e preservação da informação, verificamos que os mecanismos mais conhecidos pelos inquiridos são: a proteção de dados[2] (85.9%); o controlo de acesso[3] (78.2%); a deteção de intrusos[4] (73.9%) e a assinatura digital[5] (66.5%), Por outro lado, os mecanismos menos conhecidos são a criptografia[6] (50%) e a recuperação de desastres[7] (26%). Os resultados apurados estão dentro do esperado, dado que os mecanismos menos conhecidos envolvem processos técnicos avançados e pessoas especializadas tanto na prevenção dos riscos, como na resolução dos danos ocorridos depois de qualquer falha ou catástrofe.

Relativamente à quarta questão, relacionada com a avaliação do nível de ameaça coletiva num conjunto de atividades delituosas, constatamos que as ameaças coletivas mais expressivas aos olhos dos inquiridos são: clonagem de cartões de crédito para operações bancárias fraudulentas (M=4.06); apropriação de identidades para levar a cabo difamações e destruição do bom nome dos cidadãos (M=4.01); difusão de emails maliciosos para recolher de forma coletiva dados pessoais, bancários, médicos, etc. (M=4.01) e roubo de senhas de acesso (M=4.01). Por outro lado, existe também um nível de risco considerável para as seguintes atividades delitivas: difusão de programas maliciosos com a intenção de contornar defesas de segurança específicas, atacar clientes, subtrair informações pessoais e bancárias, entre outros objectivos (M=3.89); acesso às informações pessoais e empresariais a partir de programas do tipo *sniffers* e de pontos de acesso *wireless* que são disponibilizados como se fossem um "Free Public WiFi" (M=3.82); roubo de propriedade intelectual e espionagem de informações estratégicas como patentes, ideias de novos produtos, informações financeiras, planos de negócios, entre outras (M=3.7); acesso às informações de utilizadores que acidentalmente deixam telemóveis em táxis, pens drives em quartos de hotel, entre muitas outras situações semelhantes (M=3.67) e o comprometimento do website utilizando linhas de JavaScript que redirecionam os navegadores dos utilizadores para outros websites ou aplicações do tipo malware (M=3.64).

Em relação à quinta questão, relacionada com o nível de cultura de segurança da informação, verificamos que cerca de metade dos inquiridos considera que têm um nível de cultura de segurança da informação considerável e 23,4% consideram que detêm um nível de cultura de segurança de informação importante. Ou seja, 210 dos 284 possui um nível de cultura de segurança de informação entre um nível considerável e importante. No cômputo geral, podemos considerar que os inquiridos são sujeitos sensíveis às questões da segurança da informação, porque estão, no geral, conscientes do riscos e ameaças, bem como entendem que a segurança passa por mecanismos implementados por eles próprios, pelas empresas e pelos organismos públicos. Quando analisamos o histograma da distribuição das frequências absolutas, verificamos que o nível cultural considerável é praticamente o dobro que os níveis adjacentes, o que quer dizer que devemos continuar a investir em ações de incremento dos níveis da cultura de segurança. Estas acções de educação para a cultura de segurança são um desígnio de todos, embora passem, em primeiro lugar, pelo papel educativo da escola, como contexto expansivo desta preocupação diária na vida dos cidadãos.

Para apurar se existe alguma correlação estatisticamente significativa entre a idade dos inquiridos e o nível de cultura de segurança da informação, calculamos o coeficiente de correlação de Pearson, que mede a associação linear entre duas variáveis, onde pelo menos uma é uma escala de intervalo. Quando cruzamos as variáveis idade e nível de cultura de segurança da informação, observamos uma associação linear negativa estatisticamente significativa ($r=.155$, $p<.05$) para um nível de confiança de 95% e para as regiões críticas com uma ou duas caudas (unicaudal ou bicaudal).

Em relação à sexta e ultima questão, relacionadas com o nível de segurança na óptica dos alunos dos cloud services, constatamos que os alunos consideram a integração de processos (M=3.89), as plataformas de trabalho e produtividade (M=3.7) e o email (M=3.64) como serviços consideravelmente seguros, ainda que reconheçam os serviços relacionados com as bases de dados (M=1.69) e os serviços de armazenamento e gestão de documentos, bem como as aplicações e software como serviços com um nível de segurança

[2] Neste mecanismo são utilizados os antivírus que são programas capazes de detectar e remover arquivos ou programas nocivos.
[3] Este mecanismo permite controlar quais as pessoas autorizadas a entrar em determinado local e regista o dia e hora de acesso, controlando e decidindo as permissões de cada utilizador.
[4] Os sistemas de deteção de intrusos alertam os administradores para a entrada de possíveis intrusos nos sistemas de informação.
[5] Este mecanismo criptográfico associado a um documento que garantem a sua integridade e autenticidade. A utilização da assinatura digital prova que uma mensagem vem de um determinado emissor, porque é um processo que apenas o signatário pode realizar.
[6] A criptografia é a arte de codificação que permite a transformação reversível da informação de forma a torná-la inteligível a terceiros.
[7] As catástrofes naturais (incêndios, inundações, terramotos, entre outros) levam à necessidade de implementar planos de emergência, para garantir a preservação dos documentos e a própria integridade física dos colaboradores de uma organização.

reduzido (M=1.04). Estes resultados revelam que os utilizadores independentemente do seu nível de escolaridade, estão atentos e preocupados com a informação, documentos e aplicações que usam diariamente quando acedem e usufruem do *cloud computing*. Com base em todos os resultados do estudo, pensamos que os utilizadores universitários são sujeitos informados e capazes de reconhecerem situações de risco, o que garante uma utilização dos *cloud* service com alguma cautela e prudência no plano dos comportamentos.

CONCLUSÕES

A sociedade de informação é o resultado da promoção das comunicações e da partilha de informação, o que pode configurar, se não for devidamente acautelado, um risco à segurança ao bem-estar coletivo, à segurança individual, bem como à segurança económico-financeira das organizações. A presente investigação permite concluir que a imensa maioria dos inquiridos conhece o conceito de segurança da informação, tendo uma noção relativamente clara dos níveis de riscos assumidos nas práticas e operações diárias no uso das tecnologias de informação. Ainda neste sentido, verificamos também que existe um conhecimento considerável em torno dos mecanismos de proteção e preservação da informação, bem como uma correta avaliação do nível de ameaça coletiva de um conjunto de atividades potencialmente delituosas. Quanto à segurança da informação, o nível de cultura registado é considerável, o que de resto não deixa de ser expetável devido às características da amostra no plano da escolaridade. No plano dos *cloud services*, os utilizadores estão conscientes dos riscos inerentes do acesso remoto a documentos e aplicações.

A cultura de segurança da informação depende diretamente da participação ativa dos cidadãos, o que nos remete para o conceito de cidadania no seu estado mais dinâmico e produtivo. Este é um assunto que beneficia e afeta todos por igual medida, onde a solidariedade, a igualdade e a responsabilidade são o garante da segurança e da defesa coletiva contra *hackers* e malfeitores. Nas sociedades hiperconetadas, o desafio da privacidade e da segurança da informação é constante, complexo e interdependente, por causa da progressiva virtualização da realidade, do crescimento rápido do *cloud computing*, da explosão do fenómeno das redes sociais, da omnipresença dos dispositivos móveis e outras tecnologias emergentes, que abrem caminho e dão lugar a uma nova onda de riscos e ameaças à segurança da informação.

REFERÊNCIAS BIBLIOGRÁFICAS

Araújo, E. (2005) A vulnerabilidade humana na segurança da informação. Uberlândia.

Beal, A. (2005) Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações, São Paulo, Atlas.

OCDE (Organisation de Cooperation et de développement Économiques) (2002) Lignes directrices de l´OCDE régissant la sécurite des systèmes et reseaux d´information, Paris, Editions d´OCDE.

IT Governance Institute (2006). Information security governance guidance for boards of directors and executive management. 2ª Edição, Rolling Meadows (USA).

International Standard. Information technology -Security techniques - Information security management systems – Overview and vocabulary. Disponível em: http://www.dcag.com /images/ISO_IEC_27000.pdf

International Standard. Information technology - Security techniques - Information security management systems – Requirements. Disponível em:http://www.vazzi.com.br /moodle/pluginfile.php/135/mod_resource/content/1/ISO-IEC-27001.pdf

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011) Cloud computing: the business perspective. Decision Support Systems, 51 (1), 176-189.

National Institute of Standards and Technology –NIST (2011) The NIST definition of cloud computing. Gaithersburg, MD: NIST.

Shaikh, R., & Sasikumar, M. (2012). Security issues in cloud computing: a survey. International Journal of Computer Applications, 44 (19).