A cidadania e cultura de segurança da informação. Análise da problemática dos riscos e ameaças no plano individual e coletivo

Autores

- Galvão dos Santos Meirinhos, Prof. Dr.
- Maria Antonieta Antunes Dias, Profª. Drª.
- Francisco Manuel Lopes, Eng.
- Luís Filipe Camelo Duarte Santos, Cor.
- Maria Manuela da Costa Cardoso Gomes, Drª

RESUMO

O presente trabalho de investigação versa sobre a cidadania e a cultura de segurança da informação. A partir de um problema de conhecimento concreto, propusemo-nos conhecer a realidade de um ponto de vista exploratório, como forma de apropriação de um conjunto de realidades individuais e coletivas sobre a cultura de segurança da informação. Nesta perspetiva, lavramos um questionário adaptado aos objetivos da investigação, o que nos permitiu formular conhecimento sobre os riscos e ameaças à segurança da informação, a partir de uma amostra de 100 sujeitos, oriundos de diferentes contextos laborais. Em sentido lato, os inquiridos estão conscientes de um bom número de riscos e ameaças no plano individual e coletivo, o que prenuncia uma situação de algum conhecimento, pese embora muito haja ainda para fazer no campo da cultura de segurança. Face ao tema em epígrafe, desenvolvemos uma investigação empírica conducente à verificação e observação do fenómeno em contexto socioprofissional. Genericamente, os inquiridos conseguem definir segurança da informação, bem como reconhecer situações de risco, estando conscientes das ameaças coletivas de algumas atividades delituosas decorrentes da gestão/apropriação da informação.

Palavras-chave — Cidadania, Cultura de Segurança e Segurança da informação.

INTRODUÇÃO

Cidadania (do latim civitas, "cidade") é o conjunto de direitos e deveres que a sociedade oferece ao indivíduo. O conceito de cidadania deve ser entendido como parte determinante para a segurança individual, nacional e internacional. Este conceito permite garantir uma participação ativa dos cidadãos na promoção da segurança da comunidade, envolvida pelo poder coletivo de uma política que garanta a confiança, a manutenção e a preservação dos deveres e obrigações cívicas, sem implicar diminuição dos direitos político-sociais, bem pelo contrário, servindo para reforçar não só a intervenção social mas, sobretudo, solidificar a democracia.

Os riscos e as ameaças à segurança da informação não conhecem fronteiras, sendo cada vez mais uma preocupação global dos orgãos 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,. Sendo a segurança da informação versando a proteção de um conjunto de dados e informações com valor e em 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.

Na sociedade ocidental, a interação social e empresarial é progressivamente mediatizada por computadores que assumem um papel central na disseminação/implantação do conceito da sociedade da informação e da comunicação. Estes sistemas são cada vez mais ameaçados pelas dimensões técnicas e humanas do fenómeno da insegurança informática, que colocam a existência singular e coletiva em causa, representando sempre prejuízos e perdas dificilmente determináveis. 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.

A sociedade da informação é um projeto que marca e abrange todos os sujeitos que conformam o coletivo humano. A interconexão entre sistemas de informação é um meio de promoção das comunicações e da partilha de informação de toda e qualquer ordem, onde a descuidada partilha pode implicar um perigo efetivo ao bem-estar e à segurança individual dos cidadãos e das organizações. Com base nestes argumentos, o problema de conhecimento deste trabalho de investigação, resume-se à resposta à pergunta: será que o cidadão residente em Portugal possui uma cultura de segurança da informação? Com este propósito,

definiram-se os seguintes objetivos: analisar a problemática dos comportamentos individuais em torno da segurança de dados e informações; equacionar os impactos individuais e coletivos da existência/ausência de uma cultura de segurança da informação; apurar um índice de cultura de segurança da informação.

Um dos maiores desafios contemporâneos é saber se o cidadão 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.

DISCUSSÃO TEÓRICA

A cidadania possibilita à pessoa sentir e viver a sua liberdade individual, deixando-lhe a possibilidade de escolher e optar por um percurso de vida baseado em conceitos éticos e jurídicos onde os seus interesses pessoais se desenvolvem por valores consagrados e universalmente aceites. Fazem parte integrante destes valores fundamentais, a solidariedade, a igualdade, a liberdade e a responsabilidade, elementos exigíveis à defesa dos direitos e deveres dos cidadãos, numa comunidade que partilha um sentimento comum de justiça e humanidade. Estes fatores são essenciais à defesa e gestão criteriosa do bem público, vinculando o cidadão a um conjunto de regras que são essenciais para o desenvolvimento de uma sociedade com limites temporais e cujo percurso político-social define os critérios éticos de defesa nacional. Importa referir que a essência interpessoal entre cidadão, sociedade civil e Estado, é fundamental à manutenção de pactos e regras jurídicas, que vinculam a submissão de uma gestão político social cumpridora das normas necessárias ao bom processamento dos negócios públicos. Este conceito deve ser entendido como um bem que é de todos e que obriga a um contrato disciplinar imutável, sério, justo e soberano, cuja efetivação está acima dos interesses particulares de uma politica individual. Este pacto social entre indivíduo e sociedade tem relevância alargada, sendo a sua essência definida como um contrato que preserva a essência da justiça, identificando os homens numa politica de relação comum, constituída e alicerçada numa ética de responsabilidade em que a distribuição dos bens materiais e imateriais se fundamenta na liberdade, na distribuição equitativa e na defesa dos bens públicos destinados a servir a comunidade civil, minimizando os conflitos, assumindo o individuo uma participação ativa, responsável e de defesa pela soberania nacional.

A cidadania tem implícita a gestão criteriosa dos bens públicos , isenta e supra partidária, sendo que nenhum país triunfará se a sua sociedade não for constituída por homens honrados, inteligentes e conhecedores dos princípios básicos de defesa e gestão de todos os bens. Bens nacionais, identificados como tesouros invioláveis, cuja relação entre poder e decisão de politicas internas ou externas exige um comportamento e uma participação politico e social vocacionada para o desenvolvimento nacional e internacional, preservando o respeito dos direitos humanos e estabelecendo uma relação de combate social à fraude, à corrupção e a todos os comportamentos que violem as regras de segurança e que, no limite, coloquem em causa a Identidade, a Liberdade e a Soberania Nacional. Esta configuração espacial onde ser guerreiro é ser um cidadão combatente, assertivo e vocacionado para o sucesso do seu País e do mundo, obriga a que cada cidadão se constitua como referência para a Nação. A melhor arma politica numa sociedade democrática é alicerçada na preservação da identidade dos valores e na garantia da liberdade nacional e internacional, onde todos os cidadãos têm um papel social ativo e cuja participação é determinante para a constituição organizacional de Estados livres e seguros.

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, passando a ser um autêntico instrumento de gestão e de auditoria de informação. Por outro lado, a segurança dos sistemas e redes de informação devem 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 e, de forma antecipada, consagrar em 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 ir desde da redução funcional até mesmo à extinção da empresa. Na nossa opinião, é tudo uma questão de tempo para a instalação definitiva da cultura de segurança da informação, por causa da dependência e sobrevivência dos sujeitos e das empresas neste mundo cada vez mais ubíquo, conflituoso e inseguro. Vejamos o caso da segurança dos dados pessoais que deverão ser protegidos pelas autoridades públicas. Em Portugal, existe um Gabinete Nacional de Segurança que funciona 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 demonstra uma excelente opção, que deve ser respeitada e em caso algum violada. Existe, porém, uma exceção em que a revelação de certos dados pessoais, designadamente aqueles que estão relacionados com a saúde individual, podem e devem ser divulgados aos profissionais da área da saúde, pela importância que possam vir a ter na investigação clínica, sem os quais não seria possível obter um diagnóstico da doença. O fato de se tratar de fornecimento de informações pessoais destinadas ao serviço de uma nobre causa, como a da investigação médica, não exclui a responsabilidade de guardar o segredo como é prática corrente na

profissão de um médico consciente. Importa referir que, o profissional de saúde que recebe a informação, é um profissional idóneo, abrangido pelo segredo médico e que em circunstância nenhuma fará uso dos elementos a que tem acesso no uso exclusivo da sua atividade profissional, usando-os apenas e só, com o objetivo de um contributo destinado apenas a esclarecer e melhorar o acesso, tornando mais célere e eficaz a associação ou relação com a patologia em causa. Este procedimento estava bem salvaguardado quando existia um processo clínico individualizado e que estava na posse apenas do médico que assistia o doente e/ou a família. Porém, com a necessidade de informatização dos registos clínicos e com o fácil acesso de vários profissionais a estes dados, a confidencialidade dos mesmos está em risco. Por estas razões, não será fácil sinalizar ou responsabilizar um profissional pela divulgação de informações de caráter sigiloso e que apenas foram disponibilizadas na sequência e na necessidade de garantir uma melhor abordagem na doença.

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. Tendo em conta a situação em apreço, passaríamos a ter um registo médico cuja descodificação só seria possível efetuar, desde que o profissional de saúde tivesse em seu poder e apenas para seu uso pessoal, a correspondência exata da simbologia utilizada. É urgente dedicar algum tempo a esta reflexão, uma vez que apesar da transparência parecer ser uma excelente atitude, não podemos correr o risco de deixar o livre acesso ao conhecimento desta informação, muito menos desconhecendo quem é a que vai usar e de que forma o vai fazer quando acede aos nossos dados pessoais. Naturalmente que se tivéssemos todos uma cultura de verificação e certificação das declarações que nos são prestadas, com uma entidade receptora certificada, utilizando uma chave de acesso que permitisse guardar estes dispositivos de forma segura, este risco seria minimizado; porém no nosso dia-a-dia isto não acontece. Os registos clínicos não podem ser usados como se tratasse de um documento do tipo *Cyber Newsletter,* cuja publicação diária, recolhida e processada no âmbito do sigilo médico, possa deixar transparecer e fornecer a outras instituições dados pessoais, porque o doente nunca revelaria essa informação noutros contextos ou situações. Esta reflexão serve apenas para alertar todos os intervenientes envolvidos nesta problemática de segurança e confidencialidade dos registos clínicos. Ser assertivo e responsável é estar atento a estes detalhes, cuja subtileza com que muitas vezes nos são pedidos, podem fazer esquecer a privacidade do doente que confia e acredita que o nosso procedimento será sempre a preservação do segredo que nos foi confiado, e que não será utilizado por outra qualquer pessoa. Em suma, codificar as doenças faz parte da atividade diária do registo médico, todavia, fornecer o diagnóstico a terceiros é incorrer num crime punido por lei.

Atualmente, os padrões dos sistemas de segurança da informação estão definidos numa série de normas denominadas ISO/IEC 27000. 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 configurao 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, esta especifica 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 mantémas 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;
- Irretratabilidade – 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 contato 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, adequada para realizar um levantamento bibliográfico, bem como realizar um estudo social prévio sobre o fenómeno da cultura de segurança da informação nos cidadãos residentes em Portugal. Esta pesquisa exploratória foi realizada em contexto laboral, entre 20 e 30 de janeiro de 2014, em horário de expediente, junto de uma amostra de 100 sujeitos maiores de idade, que responderam de livre vontade e sem qualquer reserva de participação. Os questionários foram aplicados em distintos contextos laborais, nomeadamente na Universidade de Trás-os-Montes e Alto Douro, Câmara Municipal de Lamego, Comissão de Coordenação e Desenvolvimento Regional do Norte, Hospital e Regimento de Transmissões no Porto. Esta multiplicidade de contextos concorre para um estudo diversificado em termos de observações, cuja capacidade exploratória incrementa significativamente a perspetiva radiográfica do fenómeno da cultura de segurança da informação.

A exploração teórico-prática permitiu percecionar uma visão geral do fenómeno da cultura de segurança no plano da cidadania. É nossa convicção que este trabalho pode constituir uma boa base para outros consequentes, porque constatámos que poucos ou nenhuns trabalhos anteriores tiveram esta abordagem científica. Aliás e ainda neste sentido, verificamos que existe um número muito reduzido de estudos sobre a segurança da informação no plano do cidadão.

QUESTIONÁRIO

A formulação do questionário começou com a planificação e redação das distintas questões, das respostas e das escalas, onde depois de um pré-teste, levamos a cabo a sua implementação nos diferentes contextos profissionais dos membros do grupo de trabalho, finalizando o processo exploratório com a codificação e o tratamento dos dados e o consequente apuramento de resultados, mediante a aplicação de um conjunto de instrumentos de estatística descritiva e inferencial.

Neste trabalho de investigação, utilizámos um questionário estruturado, misto e autoadministrado, formado por seis questões, das quais quatro são de modalidade de resposta fechada de múltipla escolha, uma de modalidade de resposta fechada dicotómica e uma de modalidade de resposta aberta. No âmbito das escalas, foram usadas escalas de resposta psicométrica do tipo *Likert* em três questões fechadas. Quanto à estrutura do questionário, consideramos três questões sobre o conhecimento e riscos individuais de uma série de situações concretas, duas outras relacionadas com os mecanismos de proteção da informação e com as ameaças coletivas à segurança da informação, e, uma última, destinada à recolha de dados demográficos, nomeadamente o género, a idade e o nível de escolaridade do inquirido. 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 (ver questionário em anexo).

TRATAMENTO DE DADOS E DISCUSSÃO DOS RESULTADOS

A codificação e a tabulação dos dados foi levada a cabo com a aplicação SPSS Statistics 20.0 e o *Microsoft Excel*. O estudo apresenta 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 (os inquéritos tinham um código de inquiridor e número de questionário), para termos a completa noção das subamostras relacionadas com os diferentes contextos laborais. Este procedimento permite-nos fazer análises globais dos dados, bem como uma série de análises parcelares ou subamostrais, com o intuito de perceber as diferenças entre contextos laborais. A análise estatística dos dados foi iniciada pela geração das tabelas de frequências absolutas e relativas, obtendo-se a distribuição das frequências dos dados e as medidas de tendência central, nomeadamente a média[1] (M), a mediana[2] (Me) e a moda[3] (Mo). No sentido de apurar correlações entre os dados recolhidos foi calculado o coeficiente correlação de Pearson.

No plano demográfico, participaram no estudo pessoas com idades compreendidas entre os 23 e os 59 anos, sendo formada a amostra por 53 homens e 47 mulheres. Quanto ao nível de escolaridade, dois participantes possuem o mestrado, 75 a licenciatura, 20 o ensino secundário e três o ensino básico.

Em relação à questão nº1, relacionada com a definição de segurança da informação, verificamos que 80% dos inquiridos afirma corretamente que 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*. Porém, observamos 18% dos inquiridos que definiu segurança da informação como sendo o acto de *armazenar num disco um conjunto de informações, para salvaguardar os dados de um indivíduo ou de uma organização*, e 2% considerou que a segurança da informação era *imprimir um conjunto de informações...* . No âmbito da análise das sub-amostras, verificamos que o pior resultado na definição da segurança da informação é apresentado pelo Organismo de Coordenação Regional (12 respostas corretas em 20), e os melhores resultados são apresentados pelo Exército/Regimento de Transmissões-Porto, Câmara Municipal (17 respostas corretas em 20) e pela Universidade (18 respostas corretas em 20).

Em relação à questão nº2, relacionada com o nível de risco assumido pelo participante num conjunto de operações, constatamos que *Dar a conhecer e transmitir as nossas senhas de acesso* (M=4.14, Me=5, Mo=5); *Não ter um antivirus actualizado no computador* (M=3.89, Me=4, Mo=5); *Instalar software no computador de origem desconhecida ou duvidosa* (M=3.97, Me=4, Mo=5) são três operações consideradas de elevado risco pelos participantes, como podemos apurar pelos valores das medidas de tendência central anteriormente apresentados para cada operação. A seguir, existe um grupo de outras três operações classificadas entre um risco considerável e um risco relativo, nomeadamente *Abrir ficheiros que vem anexados aos emails* (M=3.41, Me=3, Mo=4); *Partilhar Pens Drives/CDs/DVDs entre amigos e colegas de trabalho* (M=3.46, Me=4, Mo=4); e *Inserir informações pessoais em formulários eletrónicos* (M=3.52, Me=4, Mo=4). E, por último, identificamos um grupo de quatro operações que os participantes consideram de risco relativo como *Abrir programas e ficheiros presentes em CDs que acompanham as publicações periódicas ou livros* (M=3, Me=3, Mo=3); *Navegar na World Wide Web (vulgo Internet)* (M=3.07, Me=3, Mo=3); *Utilizar aplicações de mensagens instantâneas* (M=3.25, Me=3, Mo=3); e *Fazer downloads/ uploads de programas e ficheiros* (M=3.36, Me=3, Mo=3).

---

[1] Média é a soma dos valores de todos os dados, dividindo a soma pelo número de dados.
[2] Mediana é o valor que separa o conjunto em dois subconjuntos de mesmo tamanho. É de extrema importância perceber que, para se calcular corretamente o valor da mediana, os elementos do conjunto devem estar em ordem do menor para o maior. Se número de elementos do conjunto for ímpar, a posição da Mediana pode ser obtida através de (n + 1)/2. Se número de elementos do conjunto for par, a mediana é a média dos dois valores centrais, cuja posição é calculada por [(n/2) + (n/2 + 1)]/2.
[3] Moda é o valor mais frequente de um conjunto de dados.

Em relação à questão nº3, relacionada com o conhecimento dos mecanismos de proteção e preservação da informação, verificamos que os mecanismos mais conhecidos pelos inquiridos são o *controlo de acesso*[4] (84%); a *assinatura digital*[5] (79%); a *proteção de dados*[6] (73%) e a *detecção de intrusos*[7] (59%). Por outro lado, os mecanismos menos conhecidos são a *criptografia*[8] (35%) e a *recuperação de desastres*[9] (26%). Os resultados apurados estão dentro do esperado, dado que os mecanismos menos conhecidos envolvem processos técnicos e pessoas especializadas tanto na prevenção dos riscos, como na resolução dos danos ocorridos depois de qualquer falha ou catástrofe.

Em relação à questão nº4, 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=4.5, Me=5, Mo=5); *Apropriação de identidades para levar a cabo difamações e destruição do bom nome dos cidadãos* (M=4.34, Me=5, Mo=5); *Roubo de propriedade intelectual e espionagem de informações estratégicas como patentes, ideias de novos produtos, informações financeiras, planos de negócios, entre outras* (M=4.3, Me=4, Mo=4); *Difusão de programas maliciosos com a intenção de contornar defesas de segurança específicas, atacar clientes, subtrair informações pessoais e bancárias, entre outros objetivos* (M=4.27, Me=4, Mo=5); *Difusão de emails maliciosos para recolher de forma coletiva dados pessoais, bancários, médicos, etc.* (M=4.23, Me=4, Mo=5); e, *Apropriação de identidades para levar a cabo difamações e destruição do bom nome dos cidadãos* (M=4.1, Me=5, Mo=5). As ameaças menos consideradas embora importantes, dado que todas as medidas de posição apresentam valores expressivos, são: *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=3.86, Me=4, Mo=4); *Acesso às informações de utilizadores que acidentalmente deixam telemóveis em táxis, pens drives em quartos de hotel, entre muitas outras situações semelhantes* (M=3.83, Me=4, Mo=4); e, *Comprometimento do website utilizando linhas de JavaScript que redirecionam os navegadores dos utilizadores para outros websites ou aplicações do tipo malware* (M=3.79, Me=4, Mo=4).

Em relação à questão nº5, relacionada com o nível de cultura de segurança da informação, verificamos que cerca de metade dos inquiridos considera que tem um nível de cultura de segurança da informação considerável (47%); contudo 29% dos inquiridos consideram que o seu nível é reduzido ou relativo (ver tabela nº1). No âmbito da análise relativa das subamostras, constatamos que os inquiridos na Câmara Municipal e no Exército apresentam os melhores resultados no que toca à cultura da segurança da informação (75% das observações localizam-se entre o nível cultural considerável e o importante), tendo como opostos os inquiridos no Hospital e na Universidade (75% das observações localizam-se entre o nível cultural relativo e o considerável).

Nível de cultura de segurança da informação...				
	Frequency	Percent	Valid Percent	Cumulative Percent
Nível cultural reduzido	3	3	3	3
Nível cultural relativo	26	26	26	29
Nível cultural considerável	47	47	47	76
Nível cultural importante	22	22	22	98
Nível cultural máximo	2	2	2	100
Total	100	100	100	

Tabela nº1 –Distribuição das frequências absolutas e relativas do *Nível de Cultura de Segurança da informação*.

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

[4] 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.
[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] Neste mecanismo são utilizados os antivírus que são programas capazes de detetar e remover arquivos ou programas nocivos.
[7] Os sistemas de deteção de intrusos alertam os administradores para a entrada de possíveis intrusos nos sistemas de informação.
[8] A criptografia é a arte de codificação que permite a transformação reversível da informação de forma a torná-la inteligível a terceiros.
[9] 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.

investir em ações de incremento dos níveis da cultura de segurança, especialmente nas questões da segurança da informação (ver gráfico nº1). Estas ações 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.

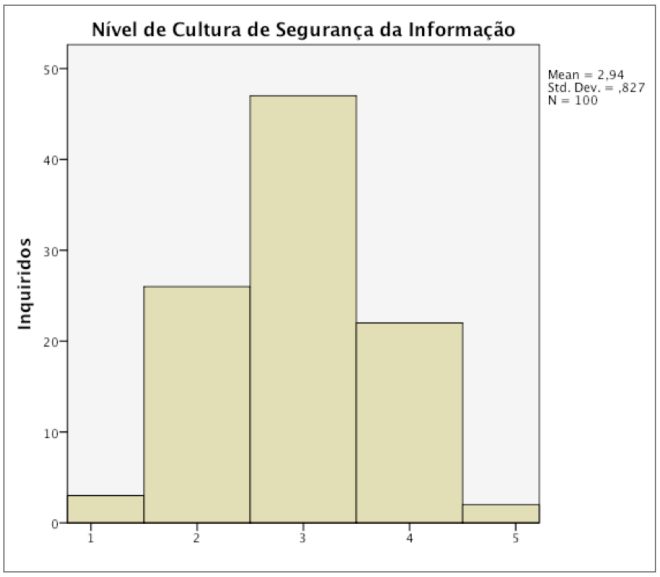

Gráfico nº1 – Histograma da distribuição das frequências absolutas do *Nível de Cultura de Segurança da informação*.
Legenda: 1. Nível Cultural Reduzido, 2. Nível Cultural Relativo, 3. Nível Cultural Considerável, 4. Nível Cultural Importante e 5. Nível Cultural Máximo.

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=-.269, p<.05) para um nível de confiança de 95% e para as regiões críticas com uma ou duas caudas (unicaudal ou bicaudal) (ver tabela nº2)

Correlations		Idade	Nível de cultura de segurança da informação
Idade	Pearson Correlation	1	-,269**
	Sig. (1-tailed)		0,003
	N	100	100
** Correlation is significant at the 0.01 level (1-tailed).			

Correlations		Idade	Nível de cultura de segurança da informação
Idade	Pearson Correlation	1	-,269**
	Sig. (2-tailed)		0,007
	N	100	100
** Correlation is significant at the 0.01 level (2-tailed).			

Tabela nº2 - Coeficiente de correlação de Pearson cruzando as variáveis Idade x Nível de Cultura de Segurança da informação.

Como a correlação apurada apresenta uma associação linear negativa, podemos então afirmar que, conforme a idade aumenta o nível de cultura de segurança da informação diminui, o que na nossa opinião, é compreensível pela sensibilidade das pessoas mais novas às tecnologias de informação e às inerentes práticas de armazenamento e proteção da informação. Porém, convém também dizer que a idade aumenta mais rapidamente que a redução do nível de cultura de segurança da informação. Ainda neste sentido, observamos também uma correlação estatisticamente significativa entre a idade e a definição de segurança da informação (r=.307, p<.05) para um nível de confiança de 95%.

Correlations		Idade	Segurança da informação
Idade	Pearson Correlation	1	,307**
	Sig. (1-tailed)		0,001
	N	100	100
** Correlation is significant at the 0.01 level (1-tailed).			

Correlations		Idade	Segurança da informação
Idade	Pearson Correlation	1	,307**
	Sig. (2-tailed)		0,002
	N	100	100
** Correlation is significant at the 0.01 level (2-tailed).			

Tabela nº3 - Coeficiente de correlação de Pearson cruzando as variáveis Idade x Segurança da informação.

Com base nestas duas correlações, seria normal verificar se existe uma correlação entre a escolaridade e o nível de cultura de segurança da informação, porém não se veio a confirmar a nossa suposição (r=.150, p=.136) para um nível de confiança de 95%. Não obstante, a investigação levada a cabo permite-nos ter uma primeira imagem de valor acrescentado sobre o fenómeno da cultura de segurança da informação. Este trabalho abre caminho a outros, que permitam estudar a realidade da segurança em extensão e em profundidade. Ainda assim, temos intenções de continuar este estudo teórico-empírico, com o intuito de o converter num estudo longitudinal, como forma de analisar no tempo as variações das questões em análise nos mesmos contextos amostrais.

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 de segurança ao bem-estar coletivo, à segurança individual, bem como à segurança económico-financeira das organizações. A presente investigação, ainda com as limitações decorrentes do tempo disponibilizado, 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 (75% dos inquiridos são licenciados).

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.

A cidadania e a cultura de segurança da informação é um daqueles temas que merece aprofundamento e curiosidade adicional por parte de académicos e investigadores. A ausência de estudos empíricos sobre cultura da segurança da informação é uma janela de oportunidades para a comunidade académica, por causa da utilidade social das investigações e do valor científico do fenómeno. Por isso, lançamos o desafio a outros investigadores, que aprofundem, indaguem e auditem o fenómeno, por forma à consagração e implementação de uma política pública de promoção da cultura de segurança da informação.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, Eduardo (2005). *A vulnerabilidade humana na segurança da informação*. Uberlândia.

BEAL, Adriana (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