REVISTA
DO ARQUIVO MUNICIPAL
DE **LAGOA**

Arade

Ano II ▸ N.º 2 ▸ 2023

REVISTA
DO ARQUIVO MUNICIPAL
DE **LAGOA**

Arade

Ficha técnica

Título: Arade. Revista do Arquivo Municipal de Lagoa

Propriedade e edição: Município de Lagoa
Largo do Município | 8401-851 Lagoa (Algarve)
Telf. 282 380 400 | E-mail: expediente@cm-lagoa.pt

Direção: Diogo Vivas

Colaboradores: Ana Lúcia Terra; Ana Margarida Dias da Silva; António Maranhão Peixoto; Armando Malheiro da Silva; Cristiana Freitas; Daniel Fernández-Carracedo; Carlos Alberto Ávila Araújo; Fernanda Ribeiro; Leonor Calvão Borges; Luís Borges Gouveia; Luís Corujo; Luis M. Hernández Olivera; Maria Beatriz Marques; Maria Clara Vieira de Andrade; Saul António Gomes; Sérgio Pratas; Silvia Cebrián Renedo.

Capa: Edifício do antigo depósito de abastecimento de água à então vila de Lagoa, construído entre 1887 e 1890, quando entrou em funcionamento e, onde, desde 2002, se encontra instalado o Arquivo Municipal de Lagoa.

Fotografia capa: Reprodução digital do postal n.º 69 da coleção de postais sobre Lagoa e o Algarve, c. 1908.

Paginação e artes gráficas: Sersilito

Impressão e acabamento: Sersilito – Empresa gráfica, Lda.

Periodicidade: Anual

Depósito legal: 503748/22

ISSN: 2795-5761

Tiragem: 300 exemplares

Data de publicação: novembro de 2023

Solicita-se permuta; Se solicita canje; On prie bien de vouloir établir l'échange; Sollicitiamo scambio; We would like Exchange; Tauschverkerhr erwünscht.

Endereço/ Adress:
Arquivo Municipal de Lagoa
Largo dos Combatentes da Grande Guerra, s/n
8400-338 Lagoa (Algarve)
Telf. 282 380 435 | E-mail: revista.arquivomunicipal@cm-lagoa.pt

REVISTA
DO ARQUIVO MUNICIPAL
DE **LAGOA**

Arade

Ano II ▸ N.º 2 ▸ 2023

Sumário

Desafios da segurança da informação: uma reflexão no contexto da ciência da informação

Information security challenges: a reflection in the information science context

Luís Borges Gouveia

◄ Imagem gerada por Luís Borges Gouveia, com recurso a IA, na aplicação *gencraft.com* com base na descrição: *"Information security challenges in the context of information science, considering both analogue and digital documents and information assets"*, Outubro de 2023.

Desafios da segurança da informação: uma reflexão no contexto da ciência da informação

Information security challenges: a reflection in the information science context

Luís Borges Gouveia
Universidade Fernando Pessoa
Centro de Investigação Transdisciplinar «Cultura, Espaço e Memória» (CITCEM)

lmbg@ufp.edu.pt
https://orcid.org/0000-0002-2079-3234

Resumo

A informação é um ativo da maior importância no contexto da sociedade atual. O seu processamento, armazenamento e comunicação, constitui parte relevante do valor que as organizações produzem, associado com o valor direto das suas atividades. Deste modo, a garantia de que a informação é integra, que se encontra protegida e, dessa forma, garante os princípios de confidencialidade adequados e, por último, que seja acessível a todos os que na organização necessitam de a obter e com os direitos de uso e exploração adequados para as diferentes formas como podem simplesmente ter o acesso, ou atualizar/alterar ou mesmo descartar a informação. A segurança da informação está assim associada com a salvaguarda destes três pilares que constituem em conjunto a proteção sobre a informação: confidencialidade; integridade e disponibilidade. Num contexto de crescente complexidade e com exigências de conetividade e integração ao nível do digital, os desafios que se colocam são significativos e importa considerar estes, ainda mais no contexto da ciência da informação e de serem asseguradas boas práticas na gestão da informação. É aqui defendido que as pessoas constituem um aspeto central para a segurança da informação, o que sustenta uma abordagem mais social e relacionada com a ciência da informação.

Palavras-chave: pessoas; informação; segurança da informação; ciência da informação.

Abstract

Information is a vital asset in today's society. It's processing, storage, and communication are a significant part of the value that organizations produce, along with their core activities. Therefore, it is essential to ensure that the information is complete, protected, and accessible to those who need it within the organization. Information security involves safeguarding these three pillars that constitute the protection of information: confidentiality, integrity, and availability. In a context of increasing complexity and digital connectivity and integration, the challenges are considerable and require attention, especially considering the field of information science and, in particular, within the promotion of good practices for information management. It is argued that people are a central issue for information security, which supports a more social and information science oriented approach.

Keywords: people; information; information security; information science.

1. Introdução

A segurança da informação é um tema cada vez mais importante na era digital, pois envolve a proteção dos dados e dos sistemas de informação contra ameaças internas e externas, como ataques cibernéticos, violações de privacidade, perdas de informação, entre outras. A segurança da informação visa garantir a confidencialidade, a integridade e a disponibilidade da informação, bem como a autenticidade, o não repúdio e a legalidade dos processos de informação.

Por sua vez, as pessoas são a componente principal das organizações, pois são elas que produzem, gerem, utilizam e partilham informação, mas também são elas que podem comprometer a segurança da informação, seja por negligência, desconhecimento ou má conduta. As pessoas devem estar conscientes e responsáveis pela segurança da informação, seguindo as políticas e normas de segurança, adotando as boas práticas e utilizando as ferramentas adequadas.

Estes primeiros parágrafos resumem o que pode ser obtido da consulta de uma fonte de informação especializada no tema da segurança da informação, que referencia os pilares da norma associada com a informação e o aspeto crítico assumido pela componente humana no processo da gestão da informação, ao assegurar o processamento, registo (armazenamento) e a troca (comunicação) de informação. No contexto dos sistemas de informação, as pessoas são tomadas como os processadores de informação, de modo a satisfazerem as suas necessidades de informação, para o suporte à tomada de decisão e como recurso essencial para a atividade realizada[1].

A ciência da informação é uma disciplina que visa estudar os fenómenos relacionados precisamente com a produção, organização, disseminação, uso e avaliação da informação, bem como considerar as tecnologias, os sistemas e os serviços de informação nesses processos[2]. Ora, neste contexto, a ciência da informação propõe uma abordagem social e centrada no uso e exploração da informação por pessoas, nomeadamente pelo estudo do comportamento informacional. Este último aspeto possibilita uma abordagem de maior profundidade para lidar com a relação entre segurança da informação e as pessoas, ao fornecer métodos, técnicas e ferramentas para gerir, analisar e avaliar dados e informação, bem como para criar soluções inovadoras e eficientes para os problemas de segurança – um desafio que constitui a contribuição maior que este texto se propõe realizar – a da oportunidade de considerar o estudo da segurança da informação e de lidar com a componente humana, por recurso à ciência da informação.

Assim, a segurança da informação, as pessoas e a ciência da informação estão intimamente relacionadas, ou pelo menos, existe um potencial a explorar para lidar com os desafios que uma maior complexidade dos sistemas atuais colocam sobre pessoas e empresas, na salvaguarda de dados e na proteção de ativos de informação. Este desafio é ainda maior, no contexto do digital, pois a sofisticação e integração a que assistimos proporciona vantagens inegáveis em custos, eficiência, eficácia, mas também desafios associados com a capacidade de pessoas e empresas asseguram níveis aceitáveis de segurança da informação.

Os pontos restantes deste texto apresentam os argumentos de suporte e desenvolvem a defesa para um relacionamento entre segurança da informação e a utilidade da ciência da informação para lidar com os desafios que são colocados face ao envolvimento

[1] GOUVEIA, Luís Borges e RANITO, João – *Sistemas de Informação de Apoio à Gestão* [Em linha]. Porto: SPI – Principia, 2004. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://spi.pt/documents/books/inovacao_autarquia/docs/Manual_VII.pdf>.

[2] GOUVEIA, Luís Borges e SILVA, Armando Malheiro da – *Método e Infocomunicação: Introdução à Dinâmica Quadripolar da Pesquisa*. Belo Horizonte: Editora Conhecimento, 2023.

de pessoas nos processos de produção, de armazenamento, de processamento e de comunicação de informação.

2. A segurança da informação

A segurança da informação é um tema cada vez mais importante na era digital, pois envolve a proteção dos dados e dos sistemas de informação contra ameaças internas e externas, como ataques cibernéticos, violações de privacidade, perdas de informação, entre outras. A segurança da informação visa garantir a confidencialidade, a integridade e a disponibilidade da informação, bem como a autenticidade, a não repúdio e a legalidade dos processos de informação, proporcionando meios de prevenção e de controlo para a sua gestão[3].

A segurança da informação é uma disciplina que abrange vários aspetos, como a gestão de riscos, as políticas e normas de segurança, os mecanismos de criptografia, os sistemas de autenticação e autorização, os sistemas de deteção e prevenção de intrusões, os planos de contingência e recuperação, entre outros. A segurança da informação é útil para proteger os ativos de informação das organizações e dos indivíduos, bem como para integrar o cumprimento de leis e regulamentos aplicáveis à proteção de dados pessoais e sensíveis, como é o caso do RGPD, Regulamento Geral de Proteção de Dados[4].

A segurança da informação é, portanto, um tema relevante e atual que requer uma constante atualização e adaptação a tecnologias emergentes, como é o caso da inteligência artificial[5] ou mesmo da computação quântica – que vem proporcionar maiores possibilidades de quebra de mecanismos de segurança em uso[6]. Em complemento há ainda a considerar os desafios que surgem no contexto da sociedade da informação[7] – nomeadamente pelo uso crescente do digital, das redes sociais e de uma organização em rede que torna mais complexa a garantia de origem e qualidade da informação utilizada, bem como dos acessos e usos associados à informação. A segurança da informação é também uma área de oportunidade para os profissionais que se dedicam ao estudo, à investigação e à aplicação das melhores práticas de segurança nos diversos domínios da informação – logo, deve constituir uma preocupação também dos profissionais da ciência da informação.

No âmbito da segurança da informação, o valor da informação é resultado das próprias caraterísticas que a informação possui. Se, por qualquer motivo, a informação altera alguma das suas caraterísticas, o valor da informação também é alterado. Normalmente, essa alteração resulta numa diminuição de valor ou mesmo perda de utilidade. Por exemplo, o exato momento em que a informação se encontra disponível é um fator crítico para os utilizadores, porque, muitas vezes, a informação perde todo o seu valor, quando não é entregue em tempo. Mesmo que os profissionais de segurança da informação e os utilizadores finais partilhem o mesmo

---

3 GOUVEIA, Luís – *Gestão da Segurança da Informação. Manual prático* [Em linha]. [Porto]: Universidade Fernando Pessoa, 2017. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://bdigital.ufp.pt/handle/10284/5954>.

4 MASCARENHAS, Raúl [*et al.*] – *Privacidade, cibersegurança e regulamentação económica. Fórum da Arrábida: repensar o futuro da Sociedade da Informação*. 15ª edição. APDSI. Convento da Arrábida. 7 de Outubro 2016.

5 MORGADO, Raul e GOUVEIA, Luís Borges – O recurso e a contribuição potencial da inteligência artificial para a cibersegurança em ambientes digitais. DIAS DA INVESTIGAÇÃO NA UFP, Porto, 2016 – *Atas* [Em linha]. Porto: Edições Universidade Fernando Pessoa, 2016, p. 185-191. [Consult. 20 set. 2023]. Disponível na WWW: URL:<http://hdl.handle.net/10284/7402>.

6 CLARKE, Richard A. e KNAKE, Robert K. – *The Fifth Domain. Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press, 2019.

7 GOUVEIA, Luís – *Sociedade da informação: Notas de contribuição para uma definição operacional* [Em linha]. Porto: Universidade Fernando Pessoa, 2004. [Consult. 20 set. 2023]. Disponível na WWW: URL:<http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf>.

entendimento das caraterísticas da informação, cada um destes grupos dá a estas caraterísticas, diferentes prioridades – a que podem corresponder diferentes sistemas de proteção[8].

Existem três aspetos associados com a informação que são bastante utilizados na prática, como referenciais, quando se procura garantir a segurança da informação e que foram introduzidos pela norma ISO 27000, de segurança da informação[9]:

- Confidencialidade: é a qualidade ou estado de prevenir exposição ou acesso não autorizado à informação, por parte de indivíduos ou sistemas. A confidencialidade da informação deve assegurar que apenas aqueles que possuem direitos e privilégios de acesso a uma informação específica é que são capazes de o fazer. Este acesso legal é muitas vezes referido por acesso autorizado e é permitido a entidades credenciadas para o efeito. A proteção de confidencialidade deve prevenir que aqueles que não devem ter acesso à informação, não o possam ganhar, por qualquer forma possível ou alternativa – evitando assim acessos indevidos. Quando indivíduos ou sistemas não autorizados puderem ganhar acesso à informação, estamos perante uma falha do sistema e pode ser afirmado que houve um comprometimento ou falha de confidencialidade. Um exemplo de quebras de confidencialidade são as mediáticas fugas de informação do segredo de justiça.
- Integridade: é a qualidade ou estado da informação em que esta constitui um todo e se encontra completa e não corrompida. Por exemplo, quando um dos seus componentes sofre uma alteração ou eliminação não detetável que não tenha sido desejada ou autorizada. Existe sempre a ameaça à integridade da informação, quando ela está exposta a modificação não autorizada, ou a corrupção ou mesmo a danificação ou outra qualquer forma de disrupção do seu estado de autenticidade. A ameaça de integridade pode ocorrer quando esta esta a ser armazenada ou transmitida.
- Disponibilidade: significa que a informação está acessível a sistemas e utilizadores autorizados, sem qualquer interferência ou obstrução e de modo a ser devidamente percebida, isto é, no formato requerido e forma de acesso que seja útil e devido para satisfação das necessidades de informação consideradas. A disponibilidade de informação assegura que apenas os utilizadores que foram verificados como tendo a autorização adequada (credenciais) para a informação é que lhes é concedido o acesso, sempre e quando o pretendam – no tempo e no espaço, ou a qualquer momento e em qualquer lugar – disponibilidade total (por vezes, a referência a altos níveis de disponibilidade requeridos é referida como alta disponibilidade e esta constitui um dos requisitos dos sistemas críticos).

Uma vez que não é possível garantir uma proteção total à informação a todas as ameaças (conhecidas e não conhecidas), torna-se necessário conduzir uma análise de risco da segurança da informação, de modo a determinar as ameaças e as vulnerabilidades para a informação e as contramedidas necessárias para serem aplicadas de modo a reduzir (mitigar) o efeito destes riscos (impacto) para um nível aceitável[10].

Deste modo, a análise de risco é um processo de identificar os ativos, os riscos para esses ativos e os procedimentos para mitigar os riscos para esses ativos. As organizações ou os indivíduos necessitam de entender quais os riscos que existem no seu ambiente de ativos de informação e como esses riscos podem ser reduzidos ou mesmo eliminados. A gestão do risco é o processo de implementar

8 GOUVEIA, Luís – *Ob. cit.*, 2017.

9 Idem.

10 Idem.

e manter as contramedidas que reduzem os efeitos do risco para um nível aceitável[11].

É da análise de risco que é obtida a informação que é necessária para a tomada de decisão relativa à segurança da informação de uma organização. Este exercício, da análise de risco, identifica os controlos de segurança, identifica as vulnerabilidades e avaliar o efeito das ameaças, para cada área ou situação de vulnerabilidade (tendo em consideração os ativos de informação identificados e identificados de acordo com a sua relevância para o contexto em análise). A gestão do risco deve ser um processo em curso, proactivo, de modo a estabelecer e manter um nível aceitável de segurança de um sistema de informação. Uma vez alcançado um nível adequado de segurança, o processo de gestão de risco monitoriza o risco nas atividades quotidianas (ou correntes) e segue os resultados da análise de risco de segurança[12].

3. Desafios no contexto digital

O contexto atual do digital e da crescente sofisticação de sistemas e redes, cada vez mais interligadas, que pode ser expresso como um ecossistema digital, no qual cada individuo tem de encontrar o seu equilíbrio e dotar-se com os meios e capacidades para aceder, gerir e gerar informação e valor, tem um impacto crescente, mesmo considerando a dimensão não digital – a analógica – sobre a qual o digital também impacta[13]. Acresce que em consideração à crescente importância do digital e da preocupação com a segurança da informação em contexto do digital, esta área tem merecido uma atenção crescente sob a denominação de cibersegurança[14].

Os desafios da segurança da informação no contexto do digital são vários e complexos, pois envolvem a proteção dos dados e dos sistemas de informação contra ameaças internas e externas, que estão em constante evolução e ganham uma sofisticação que cada indivíduo ou mesmo organização, por si próprios, não conseguem acompanhar. Estes constituem desafios que importa resolver, tal como no contexto da sociedade da informação, em rede e de forma colaborativa[15].

Uma discussão mais aprofundada das questões do digital e do seu impacto no contexto da ciência da informação é realizado por Luís Borges Gouveia e por Armando Malheiro da Silva[16]. Alguns dos principais desafios face à questão específica da segurança da informação:

- Evitar as vulnerabilidades de software, hardware e sistemas, que podem ser exploradas por elementos exteriores mal-intencionados, para invadir, roubar, alterar ou destruir dados e informação;
- Garantir a privacidade de dados pessoais e sensíveis, que podem ser recolhidos, armazenados, tratados e partilhados por

11 Idem.

12 Idem.

13 GOUVEIA, Luís Borges e SILVA, Armando Malheiro da – *Método e Infocomunicação: Introdução à Dinâmica Quadripolar da Pesquisa*. Belo Horizonte: Editora Conhecimento, 2023.

14 GOUVEIA, Luís Borges e NEVES, José Campos – O Digital e a Sociedade em Rede: contribuições para a importância de considerar a questão da (ciber)defesa. *Revista do Departamento de Inovação, Ciência e Tecnologia (DICT)* [Em linha]. N.º 5, 2014, p. 34-40. [Consult. 20 set. 2023]. Disponível na WWW: URL:<http://hdl.handle.net/10284/4605>.

15 GOUVEIA, Luís – O Conceito de Rede face ao Digital e aos Media Sociais. *Multimed. Revista do Reseau Mediterraneen de Centres d'Etudes et de Formation* [Em linha]. Porto, n.º 1, 2012, p. 85-103. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://bdigital.ufp.pt/bitstream/10284/3371/1/gouveia_87-105.pdf>.

16 GOUVEIA, Luís Borges e SILVA, Armando Malheiro da – *Ob. cit.*, 2023 e SILVA, Armando Malheiro e GOUVEIA, Luís Borges – (Des)infocomunicar ou a busca do sentido original. In LOPES, Marília dos Santos (coord.). *A História na Era da (Des)Informação*. Lisboa: CEPCEP – Centro de Estudos dos Povos e Culturas de Expressão Portuguesa; Universidade Católica Editora, 2023, p. 39-58. DOI: https://doi.org/10.34632/9789725409374

diversas entidades, sem o consentimento ou o conhecimento dos titulares;

- Sensibilizar colaboradores (internos ou externos, permanentes ou eventuais) sobre a importância da segurança da informação e as boas práticas para evitar riscos e incidentes, com recurso a politicas de segurança da informação, como o uso de senhas fortes, a atualização de antivírus, o uso de memórias como as USB pen, o cuidado com mensagens de correio eletrónico, nomeadamente o uso de ficheiros associados ou o seguimento de ligações suspeitas, entre outros;
- Lidar com as ameaças crescentes do uso e exploração do digital por entidades e pessoas, nomeadamente pelo recurso a técnicas de engenharia social que exploram a natureza humana[17];
- Reduzir o custo das soluções de segurança, que podem ser elevados para implementar e manter sistemas e ferramentas adequados à proteção dos dados e informação

Para enfrentar estes desafios, é importante adotar uma abordagem integrada e um compromisso constante com a segurança da informação, que envolva a gestão de riscos, as políticas e normas de segurança, os mecanismos de criptografia, os sistemas de autenticação e autorização, os sistemas de deteção e prevenção de intrusões, os planos de contingência e recuperação[18]. Deste modo e considerando ainda a transformação digital pela qual indivíduos e organizações estão sofrendo mudanças significativas nos seus processos e no tipo de dados e informação que possuem e que integram na sua atividade, a crescente importância das práticas individuais para com dados e informação e as competências de indivíduos ganham nova importância[19].

4. A relação com a ciência da informação

Os desafios da segurança da informação no contexto do digital são assim vários e complexos, pois envolvem a proteção dos dados e dos sistemas de informação contra ameaças internas e externas, que estão em constante evolução. A componente tecnológica é significativa, tal como a componente humana. Curiosamente, a componente associada com o recurso informação, as suas especificidades, estruturas e processos, tende a ser ou incorporada por via dos sistemas de informação na questão tecnológica ou, por via dos processos, mais associada a uma dimensão humana. Importa assim, considerar a relevância do recurso informação, ainda maior em função do digital[20].

Podemos considerar a ciência da informação como uma área interdisciplinar que abrange a criação, armazenamento, troca e uso de informação em diversas formas e contextos[21]. Deste modo, são vários os aspetos associados com a ciência da informação que podem contribuir para um aprofundamento da segurança da informação, quer em contexto individual, quer das organizações. Entre estes, especial destaque para:

17 WINKLER, Ira S. DEALY, Brian – Science Applications International Corporation. Information Security Technology?...Don't Rely on It A Case Study in Social Engineering. USENIX UNIX SECURITY SYMPOSIUM, 5, Salt Lake City – Utah, 1995 – *Atas* [Em linha]. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.usenix.org/legacy/publications/library/proceedings/security95/full_papers/winkler.pdf>.

18 GOUVEIA, Luís – *Ob. cit.*, 2017.

19 GOUVEIA, Luís – Transformação Digital: Desafios e Implicações na Perspectiva da Informação. In MOREIRA, Fernando [*et al.*] (coords.) – *Transformação Digital: oportunidades e ameaças para uma competitividade mais inteligente* [Em linha]. Faro: Sílabas e Desafios, 2017a, p. 5-28. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://ria.ua.pt/bitstream/10773/28005/1/2017_Moreira%2C%20Au-Yong-Oliveira%2C%20Gon%C3%A7alves%20e%20Costa%20-%20Transformacao%20Digital.pdf>.

20 GOUVEIA, Luís Borges e SILVA, Armando Malheiro da – *Ob. cit.*, 2023.

21 BAWDEN, David e ROBINSON, Lyn – *Introduction to Information Science*. [s. l.]: Facet Publishing, 2012.

- A análise das necessidades de informação e a organização da informação, área de trabalho específica da ciência da informação e que possui profusa literatura sobre o tema[22];
- A classificação de ativos de informação e a organização de dados. Assim, conforme descrito por Luís Gouveia[23], no contexto da Sociedade da Informação e da crescente importância da informação, importa salvaguardar o seu uso e proteger dados e informação de modo a preservar o seu valor. O processo de classificação de informação possui quatro etapas. Para a sua operacionalização é desenvolvida uma política de classificação da informação: 1, Identificar a informação como um ativo a inventariar; 2, Classificação da informação; 3, Rotulagem da informação; e 4, Manipulação e manuseio da informação – proporcionando uma descrição dos ativos de modo a selecionar os realmente relevantes e focar nestes as melhores práticas para a sua proteção;
- O *comportamento informacional*: refere as atividades que indivíduos realizam em relação às fontes e aos canais de informação, considerando as suas necessidades, buscas, usos e transferências de informação, incluindo modos de agir, sentimentos e ações envolvidos nestes processos[24]. O seu objetivo maior é o de compreender como as pessoas interagem com a informação e como essa interação as afeta, identificando os fatores que influenciam as necessidades, as buscas, os usos e as transferências de informação, procurando desenvolver modelos teóricos e metodológicos que possam explicar e prever os padrões de comportamento dos utilizadores – algo de muito útil para o contexto do uso e exploração de informação crítica e de se acautelar a segurança da informação.

5. Dos incidentes de Segurança da informação aos incidentes com pessoas como elemento central

Atendendo a um contexto mais digital e aos potenciais problemas que podem ocorrer no âmbito da segurança da informação são listados alguns dos incidentes mais relevantes em segurança da informação ocorridos na última década. Eles mostram a variedade e a gravidade das ameaças cibernéticas que podem afetar qualquer organização ou indivíduo que utilize tecnologias digitais. Destacam também a importância de implementar medidas de segurança eficazes para prevenir ou mitigar tais incidentes.

De acordo com informação pública e disponível na Web, alguns dos incidentes mais relevantes em segurança da informação nos últimos 10 anos são:

- A violação (*breach*) da *Crypto.com*, em janeiro de 2023, em que um invasor obteve acesso a 133 carteiras de criptomoedas contornando a autenticação de dois fatores (2FA) do sítio, por meio de técnicas de engenharia social[25];
- A violação (*breach*) da *Cisco*, em maio de 2022, onde um invasor conduziu uma série de ataques sofisticados de *phishing* de voz para aceder a uma conta Google de um funcionário da Cisco e depois usou as suas credenciais para aceder aos sistemas internos da Cisco[26];
- A violação (*breach*) da *News Corp*, em fevereiro de 2022, em que *hackers* infiltraram os servidores de vários meios de comunicação de propriedade da *News Corp* (ex: *The Sun*; *The Times*; e *The*

[22] ROWLEY, Jennifer e HARTLEY, Richard – *Organizing Knowledge. An Introduction to Managing Access to Information*. 4.ª ed., London: Routledge, 2008.

[23] GOUVEIA, Luís – *Ob. cit.*, 2017.

[24] SILVA, Armando Malheiro e GOUVEIA, Luís Borges – *Ob. cit.*, 2023.

[25] JENNINGS, Mike – Top data breaches and cyber attacks of 2022. *Techradarpro* [Em linha]. Pub. 5 maio 2022. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022>.

[26] Idem.

Wall Street Journal) e roubaram dados confidenciais, além de publicarem notícias falsas[27];

- A violação (*breach*) da *Microsoft*, em março de 2022, em que um coletivo de *hackers* denominado *Lapsus$* conseguiu *hackear* a *Microsoft* e comprometer o *Cortana*; o *Bing* e vários outros produtos usando credenciais roubadas de um funcionário da Microsof[28];
- A violação (*breach*) da *SolarWinds,* em dezembro de 2020, em que uma sofisticada campanha de ciberespionagem comprometeu a cadeia de fornecimento de software da *SolarWinds*, uma empresa que fornece ferramentas de gestão de rede a milhares de organizações em todo o mundo, incluindo várias agências governamentais dos Estados Unidos e empresas de dimensão mundial (Fortune 500). Os invasores inseriram códigos maliciosos em atualizações legítimas de software que lhes permitiram aceder às redes dos clientes da *SolarWinds* e roubar dados confidenciais[29];
- A violação (*breach*) da *Equifax,* em julho de 2017, em que *hackers* exploraram uma vulnerabilidade conhecida em uma estrutura de uma aplicação Web utilizada pela *Equifax*, uma das maiores agências de relatórios de crédito dos Estados Unidos, e acederam aos dados pessoais de cerca de 147 milhões de pessoas, incluindo os seus nomes, números de segurança social, datas de nascimento, endereços e números de cartão de crédito[30];
- O ataque de *ransomware WannaCry*, em maio de 2017, em que um ataque cibernético global infetou mais de 200.000 computadores em 150 países com um *ransomware* que encriptou ficheiros e exigiu pagamentos em Bitcoin para os restaurar. O ataque explorou uma vulnerabilidade no sistema operativo Windows que havia sido vazado (*leak*) da Agência de Segurança Nacional dos Estados Unidos (NSA) por um grupo chamado *Shadow Brokers*. O ataque afetou diversas organizações, como o Serviço Nacional de Saúde (NHS) do Reino Unido, a multinacional FedEx, a francesa Renault e a espanhola *Telefonica*[31];
- A violação (*breach*) da *Yahoo*, em agosto de 2013, em que *hackers* roubaram os dados de mais de um mil milhões de utilizadores da Yahoo, incluindo os seus nomes, endereços de correio eletrónico, números de telefone, datas de nascimento, senhas com *hash* e perguntas e respostas de segurança. A violação não foi divulgada até dezembro de 2016, quando a *Yahoo* revelou que havia sofrido duas grandes violações de dados, uma em 2013 e outra em 2014, que afetaram 500 milhões de utilizadores[32];
- A violação (*breach*) do *LinkedIn*, em Junho de 2012, em que *hackers* obtiveram as palavras-passe de cerca de 6,5 milhões de utilizadores do *LinkedIn* e as tornaram públicas *online*. As senhas tinham *hash*, mas sem uma sequência aleatória de dados, o que as tornava mais fáceis de serem quebradas. A violação também afetou outras plataformas de media social, como *eHarmony* e *Last.fm*[33];
- A violação (*breach*) da *Sony PlayStation Network*, em Abril de 2011, em que *hackers* invadiram o serviço de jogos *online* da Sony e roubaram os dados pessoais de cerca de 77 milhões de utilizadores, incluindo nomes, endereços, endereços de correio eletrónico, palavras-passe e detalhes de cartões de crédito. A violação também afetou a *Sony Online Entertainment* e a *Sony*

27 BROOK, Chris – The Biggest Incidents in Cybersecurity (in the Past 10 Years) (Infographic). *Fortra* [Em linha]. Pub. 18 out. 2019. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.digitalguardian.com/blog/biggest-incidents-cybersecurity-past-10-years-infographic>.

28 Idem.

29 Idem.

30 Idem.

31 Idem.

32 Idem.

33 Idem.

Pictures Entertainment. A violação resultou no desligar do serviço da *PlayStation Network* por quase um mês e custou à Sony cerca de US$ 171 milhões de dólares norte-americanos[34].

Este conjunto de incidentes tiveram um impacto real na perda de informação que devia estar protegida e que impactou as respetivas organizações com diversos graus de severidade, mas sempre com um elevado custo financeiro e reputacional.

Em complemento, poderemos considerar exemplos de incidentes de segurança da informação que não são digitais, mas de origem humana. Estes mostram como o erro humano pode levar a consequências graves para a segurança e privacidade de dados e informação. Destacam também a importância de implementar medidas de segurança eficazes para os prevenir ou mitigar:

- A violação (*breach*) do Departamento de Educação da Pensilvânia, em Outubro de 2023, em que uma falha de software no Sistema de Gestão de Informação de Professores (TIMS) expôs os dados pessoais de centenas de milhares de professores e pessoal educativo. O incidente permitiu temporariamente que indivíduos que fizeram login no TIMS acedessem a informações pessoais pertencentes a outros utilizadores, incluindo professores, distritos escolares e funcionários do Departamento de Educação. Ao todo, acredita-se que o evento de segurança tenha afetado até 360.000 professores atuais e aposentados[35];
- A violação (*breach*) do *Twitter*, em julho de 2020, em que *hackers* comprometeram as contas de várias celebridades, políticos e empresas de destaque, incluindo Barack Obama, Elon Musk, Joe Biden e Apple, e publicaram *tweets* pedindo doações em Bitcoin. O ataque foi realizado usando técnicas de engenharia social para enganar os funcionários do *Twitter* para que cedessem as suas credenciais e o acesso a ferramentas internas[36];
- A violação (*breach*) do *Marriott*, em novembro de 2018, em que *hackers* roubaram os dados pessoais de cerca de 500 milhões de hóspedes que fizeram reservas nos hotéis *Starwood*, uma subsidiária do *Marriott*. A violação foi causada por uma falha na monitorização e segurança de uma base de dados comprometida desde 2014, quando a *Starwood* foi adquirida pela *Marriott*. A violação expôs nomes, endereços, números de telefone, endereços de correio eletrónico, números de passaporte, datas de nascimento e informações do programa de fidelidade de clientes[37];
- A violação (*breach*) da *Anthem*, em Fevereiro de 2015, em que *hackers* acederam à base de dados da *Anthem*, uma das maiores companhias de seguros de saúde dos Estados Unidos, e roubaram os dados pessoais de cerca de 80 milhões de clientes e funcionários. A violação foi facilitada por um *e-mail* de *phishing* que enganou um funcionário para que ele abrisse um anexo malicioso que instalava *malware* no seu computador. O *malware* espalhou-se para outros sistemas e permitiu que aos *hackers* acederem a uma base de dados que continha nomes, números de previdência social, datas de nascimento, endereços e dados de rendimento de clientes[38];
- A violação (*breach*) da *Target,* em dezembro de 2013, em que *hackers* roubaram os dados de cartões de pagamento de cerca de 40 milhões de clientes que fizeram compras nas lojas *Target*

[34] Idem.

[35] DEURSEN, Nicole van – How to Reduce Human Error in Information Security Incidents. *Security Intelligence* [Em linha]. Pub. 13 jan. 2015. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://securityintelligence.com/how-to-reduce-human-error-in-information-security-incidents/>.

[36] ROBB, Drew – Data Breach Report Emphasizes Cybersecurity's Human Element. *SHRM* [Em linha]. Pub. 15 jun. 2021. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/data-breach-report-emphasizes-cybersecurity-human-element.aspx>.

[37] BROOK, Chris – *Ob. cit.*, 2019.

[38] Idem.

durante um período de férias. A violação foi possibilitada por um *e-mail* de *phishing* que infetou um empreiteiro de aquecimento e ar condicionado que trabalhava com a *Target*. Os *hackers* usaram as credenciais do contratante para aceder à rede da *Target* e instalar *malware* nos terminais dos pontos de venda que capturaram os dados do cartão[39].

Outros incidentes poderiam ser reportados[40]. Talvez pela sua especial relevância, importe ainda considerar três casos bem conhecidos: o caso *Snowden* e o caso *Manning* (ativismo) e o mais recente caso *Jack Teixeira* (aparente necessidade de afirmação):

- O *caso Snowden* é um escândalo de espionagem que envolveu o ex-analista da CIA e da NSA Edward Snowden, que revelou publicamente detalhes dos programas de vigilância do governo dos Estados Unidos que monitorizavam a comunicação e a privacidade de milhões de pessoas, incluindo líderes e cidadãos de outros países. Snowden vazou documentos secretos para os jornais *The Guardian* e *The Washington Post* em 2013, levando a por acusações de espionagem e roubo de propriedade do governo pelos Estados Unidos. O caso do *Snowden* gerou uma crise diplomática entre os Estados Unidos e seus aliados, além de um debate global sobre os limites da segurança nacional e os direitos à privacidade e à liberdade de expressão[41];
- O *caso Manning* é um caso de vazamento de informações secretas dos Estados Unidos pelo soldado Chelsea *Manning* (à época *Bradley Manning*). *Manning*, foi preso em 2010 por ter fornecido mais de 700 mil documentos e vídeos ao sítio Web *WikiLeaks*. Estes documentos revelavam detalhes sobre as guerras no Iraque e no Afeganistão, e sobre a diplomacia americana. *Manning* foi condenada a 35 anos de prisão por vários crimes, incluindo espionagem e roubo de propriedade do governo, sendo no entanto libertado em 2017, após o presidente Barack Obama comutar a sua pena. *Manning* é considerado um denunciante (*whistleblower*) e um ativista pelos direitos humanos por uns, e um traidor e criminoso por outros[42];
- O *caso Jack Teixeira* é um jovem (de 21 anos) que trabalhava numa base militar dos Estados Unidos e que divulgou os documentos secretos sobre a guerra na Ucrânia para impressionar os membros de um grupo *online*, no *discord*, de entusiastas por armas. Ele é descrito como racista e fanático por armas, e teria acesso a informações sensíveis sobre as operações militares dos Estados Unidos e dos seus aliados na Ucrânia, na qualidade de técnico de informática. A fuga de informação ocorreu em abril de 2023 e causou uma crise diplomática entre os Estados Unidos e os seus aliados, além de um risco para a segurança nacional. A fuga de informação ocorreu num momento de tensão entre os EUA e a Rússia, devido à guerra na Ucrânia e comprometeu fontes e os métodos de espionagem dos EUA, bem como a confiança os seus aliados, com impacto nas decisões políticas e militares dos envolvidos no conflito[43].

39 Idem.

40 CLARKE, Richard A. e KNAKE, Robert K. – *Ob. cit.*, 2019.

41 GLOBO.COM – Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. *Mundo. Globo.com* [Em linha]. Pub. 2020. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>.

42 RANGEL, Fabrício e FIGUEIRÊDO, Heitor – Wikileaks publica o primeiro dos documentos vazados por Chelsea Manning – 18 de fevereiro de 2010. *Relações Exteriores* [Em linha]. Pub. 25 de jul. 2022. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://relacoesexteriores.com.br/wikileaks-documentos-chelsea-manning/>.

43 DEBUSMANN, Bernd – Como um militar de baixa patente de 21 anos conseguiu acesso a documentos 'ultrassecretos' dos EUA. *BBC News Brasil* [Em linha]. Pub. 15 abr. 2023. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.bbc.com/portuguese/articles/c0d4ew4174vo>.

Estes incidentes ocorreram em contexto de organizações (serviços de segurança e as forças armadas dos Estados Unidos) que possuem elevados padrões associados com a segurança da informação, mas mesmo assim, foram vítimas de incidentes de elevada gravidade e que aparentemente mostraram fragilidades que exigem um aprofundamento de como evitar situações futuras associadas com pessoas, nomeadamente internas ao serviço e devidamente credenciadas.

Considerações finais

A segurança da informação é um tema muito importante na era digital, pois envolve a proteção dos dados e dos sistemas de informação contra ameaças internas e externas, como ataques cibernéticos, violações de privacidade, perdas de informação, entre outras. A segurança da informação visa garantir a confidencialidade, a integridade e a disponibilidade da informação, bem como a autenticidade e a legalidade dos processos ao lidar com dados e informação.

Para assegurar que as pessoas constituem o centro das preocupações e também o desafio na garantia da segurança da informação, é preciso adotar uma abordagem integrada e um compromisso constante com a segurança da informação, que envolva a gestão de riscos, as políticas e normas de segurança, os mecanismos de criptografia, os sistemas de autenticação e autorização, os sistemas de deteção e prevenção de intrusões, os planos de contingência e recuperação, entre outros.

Assim, para assegurar ecossistemas funcionais e capazes de responder aos desafios atuais da segurança da informação, é preciso considerar alguns aspetos de maior relevância[44], tais como:

- *Promover uma cultura de segurança da informação*: consistindo num conjunto de valores, atitudes, comportamentos e práticas que visam promover a boa consciência e a responsabilização dos indivíduos envolvidos sobre a importância da segurança da informação para os próprios, para as organizações em que colaboram e para a nossa relação com a sociedade. A cultura de segurança da informação deve ser difundida, incentivada e monitorizada pela gestão da segurança, por via da implementação de políticas, normas, treino, campanhas de sensibilização e exercícios de verificação sistemática, como é o caso das auditorias;
- *Classificar os ativos de informação*, identificando de forma clara quais os que importa proteger, em função do seu valor e do custo-benefício, tendo em consideração a eficácia das soluções encontradas;
- *Realizar exercícios de gestão de riscos*: processo de identificar, analisar, avaliar, tratar e monitorizar os riscos que podem afetar a segurança da informação. A gestão de riscos deve seguir metodologias próprias e estar focada nos contextos que respeitem os objetivos e a estratégia da organização, envolvendo as partes interessadas e considerando aspetos técnicos, humanos, organizacionais e legais;
- *Prover os controlos de segurança*: medidas de proteção que incluem desde mecanismos de criptografia, sistemas de autenticação e autorização, sistemas de deteção e prevenção de intrusões, planos de contingência e recuperação, entre outros, mais orientados para a componente humana e a sua relação com dados e informação.

Em complemento, devem ainda ser consideradas preocupações de maior grau de abstração, que importa reter enquanto princípios de modo a indivíduos e organizações possam atuar num contexto

[44] GOUVEIA, Luís – *Ob. cit.*, 2017.

de rede, de forma colaborativa e, ainda assim, respeitar preocupações de segurança da informação[45]:

- *Proteger o meio ambiente*: enquanto princípio ético que visa preservar os recursos naturais e garantir a saúde e a sobrevivência das gerações futuras. A proteção ao meio ambiente deve ser integrada na segurança da informação, pois o uso intensivo das tecnologias pode gerar impactos ambientais negativos, como o consumo excessivo de energia, a geração de resíduos eletrónicos, a emissão de gases poluentes, entre outros. A proteção ao meio ambiente deve considerar o princípio da precaução, que implica adotar medidas preventivas diante da incerteza ou da possibilidade de danos irreversíveis ao meio ambiente;
- *Garantir a privacidade* de dados pessoais e sensíveis, de negócio, bem como dados e informação que possam de algum modo impactar danos reputacionais ou de negócio a pessoas e organizações;
- *Promover a igualdade* de acesso e a conclusão, em especial por parte dos grupos desfavorecidos, de um percurso de educação e formação inclusivo e de qualidade;
- *Promover a aprendizagem ao longo da vida*, em especial através de oportunidades flexíveis de melhoria de competências e de requalificação para todos;
- *Favorecer a inclusão ativa*, com vista a promover a igualdade de oportunidades, a não discriminação e a participação ativa;
- *Reforçar a igualdade de acesso* em tempo útil a serviços de qualidade, sustentáveis e a preços comportáveis;
- *Combater a privação material* e reduzir o número de pessoas em situação de pobreza ou exclusão social;
- *Colocar as pessoas no centro das preocupações*, respeitando os seus direitos fundamentais no âmbito digital.

Deste modo, teremos uma segurança da informação que serve o individuo e as organizações, mas também a sociedade e onde se promove um uso de dados e informação mais ético e responsável.

Referências bibliográficas

BAWDEN, David e ROBINSON, Lyn – *Introduction to Information Science*. [s. l.]: Facet Publishing, 2012.

BROOK, Chris – The Biggest Incidents in Cybersecurity (in the Past 10 Years) (Infographic). *Fortra* [Em linha]. Pub. 18 out. 2019. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.digitalguardian.com/blog/biggest-incidents-cybersecurity-past-10-years-infographic>.

CLARKE, Richard A. e KNAKE, Robert K. – *The Fifth Domain. Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press, 2019.

DEBUSMANN, Bernd – Como um militar de baixa patente de 21 anos conseguiu acesso a documentos 'ultrassecretos' dos EUA. *BBC News Brasil* [Em linha]. Pub. 15 abr. 2023. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.bbc.com/portuguese/articles/c0d4ew4174vo>.

DEURSEN, Nicole van – How to Reduce Human Error in Information Security Incidents. *Security Intelligence* [Em linha]. Pub. 13 jan. 2015. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://securityintelligence.com/how-to-reduce-human-error-in-information-security-incidents/>.

GLOBO.COM – Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. *Mundo. Globo.com* [Em linha]. Pub. 2020. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>.

GOUVEIA, Luís – *Sociedade da informação: Notas de contribuição para uma definição operacional* [Em linha]. Porto: Universidade Fernando Pessoa, 2004. [Consult. 20 set. 2023]. Disponível na WWW: URL:<http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf>.

_____ – O Conceito de Rede face ao Digital e aos Media Sociais. *Multimed. Revista do Reseau Mediterraneen de Centres d'Etudes et de Formation* [Em linha]. Porto, n.º 1, 2012, p. 85-103. [Consult. 20 set. 2023]. Disponível

[45] PESSOAS 2030 (O). Programa Temático Demografia, Qualificações e Inclusão, o Pessoas 2030. *Governo de Portugal* [Em linha]. [s. d.]. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://pessoas2030.gov.pt/o-pessoas-2030/>.

na WWW: URL:<https://bdigital.ufp.pt/bitstream/10284/3371/1/gouveia_87-105.pdf>.

_____ – *Gestão da Segurança da Informação. Manual prático* [Em linha]. [Porto]: Universidade Fernando Pessoa, 2017. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://bdigital.ufp.pt/handle/10284/5954>.

_____ – Transformação Digital: Desafios e Implicações na Perspectiva da Informação. In MOREIRA, Fernando [*et al.*] (coords.) – *Transformação Digital: oportunidades e ameaças para uma competitividade mais inteligente* [Em linha]. Faro: Sílabas e Desafios, 2017a, p. 5-28. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://ria.ua.pt/bitstream/10773/28005/1/2017_Moreira%2C%20Au-Yong-Oliveira%2C%20Gon%C3%A7alves%20e%20Costa%20-%20Transformacao%20Digital.pdf>.

GOUVEIA, Luís Borges e NEVES, José Campos – O Digital e a Sociedade em Rede: contribuições para a importância de considerar a questão da (ciber) defesa. *Revista do Departamento de Inovação, Ciência e Tecnologia (DICT)* [Em linha]. N.º 5, 2014, p. 34-40. [Consult. 20 set. 2023]. Disponível na WWW: URL:<http://hdl.handle.net/10284/4605>.

GOUVEIA, Luís Borges e RANITO, João – *Sistemas de Informação de Apoio à Gestão* [Em linha]. Porto: SPI – Principia, 2004. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://spi.pt/documents/books/inovacao_autarquia/docs/Manual_VII.pdf>.

GOUVEIA, Luís Borges e SILVA, Armando Malheiro da – *Método e Infocomunicação: Introdução à Dinâmica Quadripolar da Pesquisa*. Belo Horizonte: Editora Conhecimento, 2023.

JENNINGS, Mike – Top data breaches and cyber attacks of 2022. *Techradar-pro* [Em linha]. Pub. 5 maio 2022. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022>.

MASCARENHAS, Raúl [*et al.*] – *Privacidade, cibersegurança e regulamentação económica. Fórum da Arrábida: repensar o futuro da Sociedade da Informação*. 15ª edição. APDSI. Convento da Arrábida. 7 de Outubro 2016.

MORGADO, Raul e GOUVEIA, Luís Borges – O recurso e a contribuição potencial da inteligência artificial para a cibersegurança em ambientes digitais. DIAS DA INVESTIGAÇÃO NA UFP, Porto, 2016 – *Atas* [Em linha]. Porto: Edições Universidade Fernando Pessoa, 2016, p. 185-191. [Consult. 20 set. 2023]. Disponível na WWW: URL:<http://hdl.handle.net/10284/7402>.

PESSOAS 2030 (O). Programa Temático Demografia, Qualificações e Inclusão, o Pessoas 2030. *Governo de Portugal* [Em linha]. [s. d.]. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://pessoas2030.gov.pt/o-pessoas-2030/>.

RANGEL, Fabrício e FIGUEIRÊDO, Heitor – Wikileaks publica o primeiro dos documentos vazados por Chelsea Manning – 18 de fevereiro de 2010. *Relações Exteriores* [Em linha]. Pub. 25 de jul. 2022. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://relacoesexteriores.com.br/wikileaks-documentos-chelsea-manning/>.

ROBB, Drew – Data Breach Report Emphasizes Cybersecurity's Human Element. *SHRM* [Em linha]. Pub. 15 jun. 2021. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/data-breach-report-emphasizes-cybersecurity-human-element.aspx>.

ROWLEY, Jennifer e HARTLEY, Richard – *Organizing Knowledge. An Introduction to Managing Access to Information*. 4.ª ed., London: Routledge, 2008.

SILVA, Armando Malheiro e GOUVEIA, Luís Borges – (Des)infocomunicar ou a busca do sentido original. In LOPES, Marília dos Santos (coord.). *A História na Era da (Des)Informação*. Lisboa: CEPCEP – Centro de Estudos dos Povos e Culturas de Expressão Portuguesa; Universidade Católica Editora, 2023, p. 39-58. DOI: https://doi.org/10.34632/9789725409374

WINKLER, Ira S. DEALY, Brian – Science Applications International Corporation. Information Security Technology?...Don't Rely on It A Case Study in Social Engineering. USENIX UNIX SECURITY SYMPOSIUM, 5, Salt Lake City – Utah, 1995 – *Atas* [Em linha]. [Consult. 20 set. 2023]. Disponível na WWW: URL:<https://www.usenix.org/legacy/publications/library/proceedings/security95/full_papers/winkler.pdf>.

ISSN 2795-5761

Lagoa DO ALGARVE

Lagoa 250

arquivo municipal de Lagoa