Fall 10-16-2021

From information security to data protection: proposal for a reference model

António Gonçalves
INESC-ID, agoncalveslx@gmail.com

Anacleto Correia
Escola Naval/CINAV, anacleto.correia@gmail.com

Da segurança da informação à proteção dos dados: proposta de um modelo de referência

From information security to data protection: proposal for a reference model

António Gonçalves, IPS, INESC-ID, Portugal, agoncalveslx@gmail.com

Anacleto Correia, Escola Naval/CINAV, Portugal, anacleto.correia@gmail.com

Resumo

O termo proteção de dados é frequentemente associado indistintamente ao termo segurança da informação. Este artigo contrapõe que, embora exista uma relação entre segurança da informação e proteção de dados, estes dois conceitos não são análogos. Além disso, o artigo argumenta que a proteção de dados ultrapassa os limites da segurança da informação para incluir não só a proteção dos recursos de informação, mas também inclui outros aspetos como a segurança do tratamento da informação. Na segurança da informação, o objetivo é proteger os recursos de uma organização, tais como informação, hardware e software informático. Na proteção de dados, as organizações têm de seguir regras rigorosas denominadas "princípios de proteção de dados". Esta dimensão adicional tem implicações para a organização. Por exemplo, determina que se faça uma utilização adequada da informação sobre indivíduos. Neste trabalho será feito um esforço para incluir na abordagem CIA os atributos de proteção de dados.

Palavras-chave: segurança de informação; proteção de dados; dados pessoais; proteção do tratamento.

Abstract

The term data protection is often used interchangeably with the term information security. This article argues that while there is a substantial overlap between information security and data protection, these two concepts are not analogous. Furthermore, the article argues that data protection goes beyond the boundaries of information security to include not only the protection of information resources, but also includes other aspects such as the security of information processing. In information security, the aim is to protect an organisation's resources, such as information, computer hardware and software. In data protection, in addition to maintaining information security, organisations have to follow strict rules called "data protection principles". This additional dimension has implications for the organisation. For example, it requires that proper use is made of information about people. In this paper an effort will be made to include data protection attributes in the CIA approach.

Keywords: *information security; data protection; personal data; protection of processing.*

1. INTRODUÇÃO

Ao longo das últimas décadas, os avanços na Tecnologia mudaram radicalmente as nossas vidas. Podemos aceder a uma variedade de serviços e informações em qualquer lugar, a qualquer momento. Embora estes avanços tenham trazido enormes benefícios, o desenvolvimento da Tecnologia da Informação também teve um impacto significativo na privacidade dos utilizadores. De facto, cada

vez mais informação pessoal é recolhida, processada, partilhada e divulgada. Existem várias razões para a recolha, partilha e divulgação de informações pessoais. Por exemplo, organismos públicos, podem partilhar os seus dados para fins de investigação ou estatísticos e organismos privados podem tratar os dados dos seus clientes para prestarem serviços de forma mais eficiente e eficaz (Castells, 1996).

Contudo, o armazenamento, o tratamento e a divulgação ou partilha de dados pessoais, coloca diversos desafios de segurança relacionados com a privacidade dos indivíduos: Como deve ser definida uma política de privacidade e como alinhá-la com a política de segurança de informação? e como deve ser gerido o risco associado a manipulação dos dados pessoais?

Por outro lado, o conceito de privacidade é distinto em diferentes países, culturas ou jurisdições. A definição adotada por Organização para a Cooperação e Desenvolvimento Económico (OCDE) é "qualquer informação relativa a um indivíduo identificável (sujeito dos dados)". Outra definição, adotada no espaço europeu, é o regulamento RGPD que estende o conceito anterior, incluindo os direitos e obrigações dos indivíduos e das organizações no que diz respeito a recolha, utilização, retenção e divulgação de dados que podem ser relacionados com pessoas. Podemos afirmar, em termos gerais, a privacidade está associada à recolha, utilização, divulgação, armazenamento e destruição de dados pessoais, ou seja, está associada ao ciclo de vida dos dados, desde a geração até à destruição dos dados. (O'Leary et al., 1995) (Dibble, 2020).

Podemos ainda afirmar que a privacidade da informação é o interesse que uma pessoa tem em controlar, ou pelo menos influenciar significativamente, o tratamento de dados sobre si próprio durante o ciclo de vida dos dados, incluindo assim a definição de Clarke (Clarke, 1999).

Associado à segurança de informação existe um processo de gestão do risco que consiste em identificar os riscos, avaliar a probabilidade da sua ocorrência, e tomar medidas para reduzir o risco a um nível aceitável. Todos os processos de análise de risco utilizam a mesma metodologia: determinar o ativo a ser revisto; identificar o risco, questões, ameaças ou vulnerabilidades; avaliar a probabilidade da ocorrência do risco e o impacto para o ativo ou para a organização caso o risco se concretize; finalmente, identificar os controlos que levariam o impacto a um nível aceitável (Purdy, 2010).

Relativamente a segurança da informação podemos afirmar como sendo a proteção da informação e dos seus elementos críticos, incluindo os sistemas e hardware que utilizam, armazenam e transmitem essa informação. Whitman identifica várias características críticas da informação que lhe conferem valor nas organizações, nomeadamente a confidencialidade, integridade e disponibilidade da informação (Whitman & Mattord, 2012).

É importante notar que, no caso da segurança da informação, a informação é o bem que deve ser protegido e no caso da privacidade da informação o bem que deve ser protegido é o controlo da informação pessoal, utilizada pelas organizações, por parte do seu proprietário. Por isto conseguir conjugar a segurança da informação com a privacidade da informação é um desafio relevante e que ainda necessita de ser clarificado.

Em ambos os casos a gestão do risco é um processo que inclui um conjunto de atividades coordenadas realizadas para dirigir e controlar o risco de perda de disponibilidade, confidencialidade e integridade da informação organizacional e a perda do controlo da informação pessoal por parte do seu proprietário. Inclui um conjunto de planos, relações, responsabilidades, recursos, processos que fornecem a política e os objetivos para gerir o risco. A política de gestão do risco aborda os objetivos e a estratégia da organização relativamente à gestão do risco (Kenyon, 2020).

Este artigo está organizado da seguinte forma: Secção 2 dá uma breve descrição do que é exatamente a segurança de informação. A Secção 3 discute a segurança dos dados e questões de proteção da privacidade associadas ao longo de todas as fases do ciclo de vida dos dados. A secção 4 apresenta um modelo de segurança que incluiu a segurança da informação e da proteção dos dados. A Secção 5 apresenta uma discussão sobre o tema. A Secção 6 descreve o trabalho de investigação futuro.

2. INFORMAÇÃO E SEGURANÇA DE INFORMAÇÃO

A informação pode apresentar numerosos formatos e ser utilizada de diferentes modos. Pode ser em papel, em formato eletrónico, transmitida por correio ou por meios eletrónicos, exibida em filmes, transmitida em conversação, etc. Associada a informação existe ainda o conceito de confidencialidade da informação. Por exemplo, para um documento limitado apenas ao uso interno, a sua proteção tem alta confidencialidade, enquanto que para o documento disponível ao público, a sua confidencialidade é baixa (Von Solms & Van Niekerk, 2013).

O estado, a forma e a localização da informação pode mudar inúmeras vezes durante o seu ciclo de vida, enquanto que a confidencialidade à informação muda com menos frequência. Consequentemente, devem ser aplicadas medidas de segurança diferentes às informações de diferentes níveis de confidencialidade: um documento comercial normal pode ser enviado por correio normal, enquanto que um documento confidencial só deve ser enviado por entrega especial (Von Solms & Van Niekerk, 2013).

2.1. Objetivo da segurança de informação

O objetivo da segurança da informação é proteger os recursos de uma organização, tais como informação, hardware e software. Através da seleção e aplicação de salvaguardas apropriadas, a segurança ajuda a organização a cumprir os seus objetivos ou missão empresarial, protegendo os

seus recursos físicos e financeiros, reputação, posição legal, funcionários e outros ativos corpóreos e incorpóreos (Peltier, 2013) .

A segurança da informação, atualmente, não é um produto, ou uma tecnologia, mas um processo. A segurança da informação era uma questão estritamente técnica. No entanto, à medida que a utilização de computadores e redes evoluiu, o processo de segurança destes computadores e redes também teve de evoluir para se estender para além apenas do aspeto técnico. O processo de segurança da informação pode exigir a utilização de certos produtos, mas não é algo que possa ser obtido de uma prateleira (Mitnick & Simon, 2003) (Wood, 2004).

Por exemplo, se a segurança da informação for encarada como uma questão estritamente técnica, é necessário cuidar do processo de segurança técnico. No entanto, é necessário evoluir de modo a ir apenas para além das questões técnicas.

2.2. Propriedades da segurança de informação

Quando abordamos a segurança da informação é importante avaliar as propriedades que deve ter. Essas propriedades incluem a disponibilidade, confidencialidade, e integridade da informação. A disponibilidade refere-se ao facto de as informações utilizadas por uma organização serem acessíveis quando são necessárias. A confidencialidade refere-se à restrição do acesso à informação àqueles que estão autorizados. A integridade refere-se à correção da informação armazenada e manipulada (Andress, 2014).

2.3. Risco e segurança de informação

Podemos definir o risco de segurança da informação como o efeito da incerteza devido a algo adverso acontecer (um evento) e que pode afetar o valor da informação. Este acontecimentos podem dificultar a realização dos objetivos da organização e pode provocar perda do valor do negócio (Peltier, 2013).

A segurança da informação é necessária porque os eventos adversos podem acontecer na tecnologia que suportam à informação (i.e., no armazenamento, transmissão, edição, copia, etc..) e que pode criar riscos provocada por brechas nos sistemas de suporte. Uma brecha num sistema pode afetar a informação e consequentemente pode provocar perda para o seu proprietário, quer sejam reconhecidas ou não. A perda pode ser direta (através da redução do valor da informação) ou indireta (através interrupção do serviço). A perda traduz-se em prejuízo para a reputação do proprietário da informação, redução de vantagem competitiva, responsabilidade legas, etc.) (Blakley, McDermott, & Geer, 2001) .

A gestão do risco de segurança da informação é um processo permanente de desafio que permite compreender os potenciais riscos para os valiosos ativos de informação da organização e as ferramentas para os abordar (Purdy, 2010).

3. DADOS PESSOAIS, PROTEÇÃO DE DADOS E SEGURANÇA DO TRATAMENTO

Dados pessoais é todo a informação sobre uma determinado pessoa física. Pode ser qualquer pessoa, incluindo um cliente, funcionário, parceiro, membro, apoiante, contacto comercial, funcionário público ou membro do público. Não precisa de ser informação 'privada' - mesmo informação que seja do conhecimento público ou que seja sobre a vida profissional de alguém podem ser dados pessoais. Não cobre informação verdadeiramente anónima - mas se ainda assim for possível identificar alguém a partir dos detalhes, ou combinando-a com outra informação, continuará a contar como dados pessoais. Só inclui documentos em papel se projetar colocá-los num formato digital ou arquivá-los de forma organizada (Sharma & Menon, 2020).

3.1. Proteção de dados

A proteção de dados é a utilização justa e adequada da informação sobre as pessoas. Faz parte do direito fundamental à privacidade - mas, a um nível mais prático, trata-se realmente de criar confiança entre pessoas e as organizações. Trata-se de tratar as pessoas de forma justa e aberta, reconhecendo o seu direito a ter controlo sobre a sua própria identidade e as suas interações com os outros, e de encontrar um equilíbrio com os interesses mais vastos da sociedade.

3.2. Tratamento de dados

Quase tudo o que faz com dados conta como tratamento de dados; incluindo a recolha, gravação, armazenamento, utilização, análise, combinação, divulgação ou eliminação de dados pessoais. Compreender o papel de uma organização em relação aos dados pessoais que está a processar é crucial para assegurar o cumprimento da segurança do tratamento. As obrigações, no âmbito da proteção do tratamento, variam dependendo de ser um responsável pelo tratamento ou um subcontratante. O facto de ser controlador ou processador depende de uma série de questões. A questão-chave é - quem determina as finalidades para as quais os dados são processados e os meios de processamento. As organizações que determinam as finalidades e os meios de tratamento serão os responsáveis pelo tratamento, independentemente da forma como são descritos em qualquer contrato sobre serviços de tratamento (Lin & Kifer, 2014).

3.3. Regulamento geral de proteção de dados

O Regulamento Geral de Proteção de Dados (RGPD) é constituído por um conjunto de regras para alcançar a privacidade das pessoas no tratamento dos seus dados pessoais e na circulação desses

dados. Quando essas regras são consideradas no funcionamento dos sistemas de informação, aquela torna-se exequível para aprovação legal dentro desse âmbito. O modelo serve o propósito de analisar as empresas no que diz respeito à utilização dos dados pessoais do sujeito, permitindo captar e melhorar as capacidades de proteção de dados colocadas no RGPD (Dibble, 2020).

3.4. Segurança do tratamento

No âmbito do RGPD podemos definir a segurança do tratamento se se verificar cumulativamente um conjunto de propriedades que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas. As propriedades englobam a licitude, lealdade e transparência das operações realizadas sobre os dados. existe a limitação das finalidades, ou seja, os dados são recolhidos para finalidades bem definidas e autorizadas não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades. Uma vez reunidos os dados devem permanecer exatos e atualizados sempre que necessário e deve, ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados (Dibble, 2020).

4. MODELO CONCEPTUAL DA SEGURANÇA DE INFORMAÇÃO E PROTEÇÃO DE DADOS

A informação é um ativo empresarial de importância permanente em todas as organizações. Por conseguinte, deve ser protegida como qualquer outro bem de valor. Este é o objetivo da segurança da informação, e um modelo de segurança da informação proporciona este tipo de proteção para os recursos de informação de uma empresa.

No suporte ao modelo de segurança informática tem sido utilizada a tríade da CIA, cuja sigla resulta dos atributos: confidencialidade, integridade e disponibilidade. A sua origem surge com Saltzer e Schroeder os quais afirmaram que, os especialistas em segurança distinguem três categorias de ameaças à informação: divulgação não autorizada de informação (confidencialidade), modificação não autorizada de informação (integridade) e negação não autorizada de utilização (disponibilidade) (Saltzer & Schroeder, 1975).

A tríade CIA, tem sido integrada em modelos, dos quais destacamos o modelo de McCumber, também conhecido por cubo de McCumber, a extensão proposta por Maconachy e a abordagem proposta por Parker e por fim o modelo preconizado pela família das normas ISO 27000.

O modelo de McCumber propõe uma abordagem orientada aos mecanismos de segurança associando a 3 dimensões, a saber, as propriedades da informação (tríade CIA- confidencialidade, integridade e disponibilidade), os estados da informação (armazenamento, transmissão e no processamento) e as medidas da segurança (tecnologia, política e práticas, e educação, formação e

sensibilização). Maconachy estende o cubo McCumber ao introduzir a dimensão tempo e serviços de segurança adicionais (autenticação e não repudiação). Parker sugere um novo modelo que consiste em seis elementos fundamentais: a disponibilidade, utilidade, integridade, autenticidade, confidencialidade e posse.

Em termos de estratégia os modelos de segurança procuram identificar os principais conceitos baseado na análise do risco e integra a tríade CIA numa estratégia baseada no risco. Com base neste pressuposto é apresentado o modelo da Figura 1 o qual integra os conceitos de proteção de dados.

Podemos identificar os seguintes artefactos: recurso, vulnerabilidade, ataque, risco, contramedidas, violação de segurança de informação e de proteção de dados.

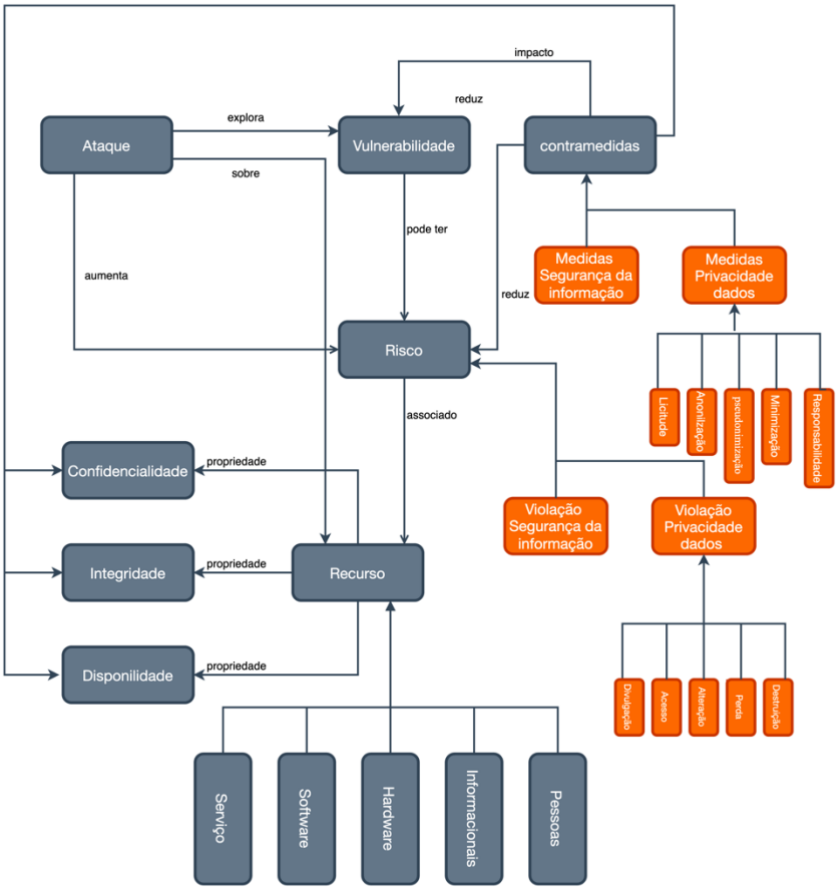

Figura 1 – Modelo de Segurança de Informação e Proteção de dados.

4.1. Vulnerabilidade

Um sistema de informação é mais do que hardware e software; inclui as políticas, procedimentos, e organização sob os quais esse hardware e software é utilizado. As falhas na segurança podem surgir de qualquer uma destas áreas ou de qualquer combinação destas áreas. Assim, faz pouco sentido restringir o estudo de vulnerabilidades a problemas de hardware e software (Probst, Hunker, Bishop, & Gollmann, 2010).

Uma vulnerabilidade é uma fraqueza (lapsos em procedimentos, tecnologia ou gestão (ou alguma combinação destes fatores) que pode ser explorada por um atacante sobre um recurso, com o intuito de violar a política de segurança de informação ou de proteção dos dados. A utilização dessa falha para violar a política de segurança do sítio chama-se exploração da vulnerabilidade.

A gestão da vulnerabilidade contém processos comuns que incluem: descobrir todos os recursos, avaliar as suas vulnerabilidades. As vulnerabilidades podem ser mitigadas através do uso de contramedidas que reduz o risco para os recursos.

Os sistemas de informação das organizações e a sua infraestrutura informática subjacente contêm vulnerabilidades que podem ser exploradas por várias entidades, internas ou externas. As organizações utilizam tecnologias de segurança para reduzir o risco de danos apresentados por estas vulnerabilidades (Purdy, 2010).

4.2. Risco

O risco de segurança da informação e da proteção de dados, ou seja, o efeito da incerteza devido a algo adverso que ocorre é uma especto relevante, e diz respeito à forma como uma organização encara os desafios que enfrenta, sendo para tal necessário delinear os limites da gestão de riscos dentro da organização. Isto porque a sobreavaliação como a como a sobrestimação do valor dos recursos são práticas perigosas na avaliação do risco. Em termos gerais podemos afirmar que com a introdução do conceito do risco pretendemos responder as seguintes questões: Que recursos temos de proteger? Como é que esses recursos são ameaçados? e o que podemos fazer para combater essas ameaças? (Peltier, 2013).

A avaliação de risco fornece uma forma sistemática para a organização obter uma visão abrangente dos riscos existentes e as suas consequências, e as contramedidas para lidar com eles. Uma vez que o processo de avaliação inclui os riscos associados a todo o tipo de plataformas, sistemas operativos, programas de aplicação, redes, pessoas, e processos, bem como as interdependências entre eles, é um processo desafiante e, na maioria dos casos, as organizações necessitam de ajuda externa para o executar adequadamente. Note-se que os erros na avaliação do risco podem ser perigosos e dispendiosos. Subestimar os riscos pode deixar a organização vulnerável a ameaças graves. Para isto o modelo associa o risco as violações de segurança de informação e as violações da privacidade dos dados.

4.3. Contramedidas

Uma salvaguarda de segurança da informação (controlo ou contramedida) é uma atividade procedimental ou técnica utilizado para reduzir o risco para os recursos da organização, minimizando assim qualquer perda potencial. As salvaguardas podem envolver ações de prevenção, deteção ou

correção. Para responder a qualquer risco inaceitável que não possa ser evitado ou transferido para outra parte, deve ser implementada uma proteção adequada (atenuação do risco). As boas práticas classificam as salvaguardas de segurança da informação em cinco categorias: autenticação, controlo de acesso, confidencialidade dos dados, integridade dos dados e não repudiação (Peltier, 2013).

4.4. Monitorização da segurança

A monitorização contínua desempenha um papel importante no domínio da segurança da informação e proteção de dados. Para quase todas as normas, metodologias ou modelos de segurança da informação, existe algum tipo de monitorização ou avaliação que deve ser realizada regularmente, e os resultados precisam de ser cuidadosamente documentados. Nesta fase o processo de implementação deve ser monitorizado para assegurar a sua correção e que verifica: i) Os custos de implementação e os recursos utilizados ficam dentro dos limites identificados; ii) se as contramedidas são corretamente implementadas conforme especificado no plano, a fim de que a redução do nível de risco identificado é alcançada e iii) se os controlos são operados e administrados conforme o necessário.

Nesta fase, as eficácias dos processos de gestão de risco podem ser asseguradas, bem como o alinhamento das respostas de risco planeadas com as missões, regulamentos governamentais, políticas, normas e diretrizes da organização (Peltier, 2013).

5. DISCUSSÃO

Os modelos de segurança e proteção procuram evitar um conjunto de violações que podem ocorrer nas seguintes circunstâncias: (1) A informação pessoal, quando combinada com conjuntos de dados externos, pode levar à inferência de novos factos sobre os utilizadores. Esses factos podem ser reservados e não devem ser revelados a terceiros; (2) A informação pessoal é por vezes recolhida e utilizada para acrescentar valor ao negócio. Por exemplo, os hábitos de compra do indivíduo podem revelar muitas informações pessoais; (3) Os dados sensíveis são armazenados e tratados num local que não possui as medidas de proteção adequadas e pode ocorrer fuga de dados durante as várias fases de tratamento.

As violações de privacidade de dados podem ser amplificadas por brechas (i.e., violações de segurança de informação) no sistema que pode afetar os atributos CIA e na sensibilidade da informação e consequentemente pode provocar perda para o proprietário da informação, quer sejam reconhecidas ou não.

Os modelos de segurança e privacidade procuram obter um equilíbrio entre as medidas de controlo e a ausência delas. Por exemplo, a implementação de controlos de segurança pode introduzir muitas

complexidades a uma organização. Estas complexidades podem levar a erros ou dificultar a deteção de atividades não autorizadas e podem por vezes criar uma fraqueza inadvertidamente.

Por exemplo, quanto mais granuloso e complexo for o seu conjunto de regras de acesso, podemos ser levados a pensar que estamos a aperfeiçoar a postura de segurança da organização com restrições detalhadas de acesso (princípio do privilégio mínimo), mas fazendo-o também aumenta a possibilidade de cometer um erro de lógica que pode abrir um inesperado buraco no seu perímetro de controlo. Estas são compensações que têm de ser pesadas e feito todos os dias como um líder de segurança da informação.

De acordo com Wheller (Wheeler, 2011) podemos utilizar os princípios de Saltzer e Schroederh (Saltzer & Schroeder, 1975) para influenciar muitas facetas da segurança, tais como normas, diretrizes, e desenhos de controlo. São eles: privilégio mínimo (não devem ser permitidas comunicações ou atividades a menos que haja uma necessidade explícita para essa transação ou acesso), defesa em profundidade (utilização de múltiplas técnicas de segurança ou camadas de controlos para ajudar a reduzir a exposição se um controlo de segurança for comprometido ou contornado) e separação de privilégios (nenhuma pessoa tem autoridade para desempenhar todas as funções privilegiadas, especialmente todas as funções relacionadas com a criação e tratamento de informação sensível ou crítica).

6. CONCLUSÕES

As práticas e desafios da integração dos requisitos de segurança de informação e proteção de dados nas organizações ainda é uma área relativamente inexplorada de investigação.

Neste artigo, analisamos os principais conceitos da segurança de informação e de proteção de dados e concentrámo-nos em propor um artefacto integrador dos conceitos através dos atributos CIA. Procuramos ainda integrar os conceitos de violação de segurança de informação com o conceito de violação de proteção de dados. Dois conceitos relacionados, mas distintos que pode inclusive existir uma violação dos dados pessoais e não haver uma violação de segurança de informação.

Neste artigo, ilustramos as definições sintática de proteção de dado que engloba o tratamento dos dados o ciclo de vida dos dados, utilizados para impedir a divulgação de identidade dos donos dos dados pessoais. Também apresentámos uma visão geral de um modelo integrador de segurança de informação e proteção de dados.

REFERÊNCIAS

Andress, J. (2014). The basics of information security : understanding the fundamentals of InfoSec in theory and practice. Retrieved from http://www.books24x7.com/marc.asp?bookid=66986

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk

management.
Castells, M. (1996). *The information age* (Vol. 98). Oxford Blackwell Publishers.
Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67.
Dibble, S. (2020). *GDPR*.
Kenyon, B. (2020). ISO 27001 Controls - A guide to implementing and auditing. IT Governance Publishing Boston. Retrieved from https://learning.oreilly.com/library/view/-/9781787782402/?ar
Lin, B.-R., & Kifer, D. (2014). A first principle approach toward data privacy and utility. [University Park, Pa.]: Pennsylvania State University. Retrieved from https://etda.libraries.psu.edu/paper/21497/
Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.
O'Leary, D. E., Bonorris, S., Klosgen, W., Khaw, Y.-T., Lee, H.-Y., & Ziarko, W. (1995). Some privacy issues in knowledge discovery: the OECD personal privacy guidelines. *IEEE Expert*, *10*(2), 48–59.
Peltier, T. (2013). *Information Security Fundamentals, 2nd Edition*. Auerbach Publications. Retrieved from https://books.google.pt/books?id=XpB-zQEACAAJ
Probst, C. W., Hunker, J., Bishop, M., & Gollmann, D. (2010). *Insider threats in cyber security* (Vol. 49). Springer.
Purdy, G. (2010). ISO 31000:2009 - Setting a new standard for risk management: Perspective. *Risk Analysis*, *30*(6), 881–886. https://doi.org/10.1111/j.1539-6924.2010.01442.x
Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems A . Considerations Surrounding the Study of Protection. *Access*, *63*(9), 1278–1308. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1451869
Sharma, S., & Menon, P. (2020). Data privacy and GDPR handbook. Retrieved from https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=5986738
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
Wheeler, E. (2011). Security Risk Management: Building an Information Security Risk Management Program from the Ground Up.
Whitman, M. E., & Mattord, H. J. (2012). *Roadmap to information security: For IT and infosec managers*. Cengage Learning.
Wood, C. C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security*, *2004*(1), 16–17.