GESTÃO DA INFORMAÇÃO

Temas e Abordagens

Autores

- Adriana Peixe
- Eduardo Lauer
- Jorge Balsan
- Josias Corecha
- José Simão
- Larissa Benck
- Marcio Santos
- Marilyn Cyganczuk
- Michel Santos

Programa de Pós-Graduação em Gestão de TI (PPGGI)

2019

ADRIANA MARIA MIGUEL PEIXE
JORGE BALSAN
JOSÉ SIMÃO DE PAULA PINTO
MARCIO RODRIGO SANTOS
(Coordenadores)

Gestão da Informação:

Temas e Abordagens

Autores:
Adriana Maria Miguel Peixe
Eduardo Lauer
José Simão de Paula Pinto
Josias Farias Corecha
Jorge Balsan
Larissa Lourenço Nunes Benck
Marcio Rodrigo Santos
Marilyn de Souza Cyganczuk
Michel Cesar dos Santos

CURITIBA

2019

Bibliotecário: Eduardo Silveira – CRB 9/1921

Gestão da Informação : temas e abordagens / Adriana Maria Miguel Peixe [et al]. - 2019.
53 p.

ISBN: 978-85-7335-338-9

Autores: Adriana Maria Miguel Peixe, Eduardo Lauer, Jorge Balsan, Josias Corecha, José Simão Pinto, Larissa Benck, Marcio Santos, Marilyn Cyganczuk, Michel Santos.

1. Gestão da informação. 2. Gestão do conhecimento. I. Autor. II. Título.

CDD 658.4038

Gestão da Informação

Sumário

1. Introdução

Existem várias definições para dados, informação e conhecimento, nenhuma de aceitação universal, quase sempre levando à questão de que "o conhecimento é a informação contextualizada, e que esta é a contextualização dos dados" (conforme Braman, S. ***Defining Information****: an approach for policymakers*. *Telecommunications Policy*, 13, 1989).

Continuando nesta busca, uma referência que leva à norma ISO-IEC-2382 informa o significado de dado (*data*), que é a "representação de fatos ou ideias de maneira formalizada e capaz de ser comunicada ou manipulada por algum processo" e de informação (information): "em processos automáticos de processamento de dados, o significado que os humanos atribuem aos dados a partir de convenções conhecidas usadas em sua representação".

De forma geral, temos que os dados representam os valores brutos ou não tratados, como por exemplo o local de nascimento de uma pessoa, e as informações são os valores tratados ou agrupados de forma a produzir dado extra, de forma sumarizada, como por exemplo quantas pessoas nasceram em certo local.

Mas, o que é a Gestão da Informação?

O *Free On-Line Dictionary of Computing* (disponível em: http://wombat.doc.ic.ac.uk), oferece uma definição para a gestão da informação: "*information management is the planning, budgeting, control and exploitation of the information resources in an organization. The term encompasses both the information itself and the related aspects such as personnel, finance, marketing, organization and technologies, and systems. Information Managers are responsible for the coordination and integration of a wide range of information handling activities within the organization. These include the formulation of corporate information policy, design, evaluation and integration of effective information systems services, the exploitation of information technologies for competitive advantage and the integration of internal and external information and data*".

Temos ainda a definição dada pelo *Information Resource Management Manual*, da *Environmental Protection Agency* (EPA - 1972, EUA) de que a Gestão da Informação é o "conjunto de atividades que proporcionariam o planejamento, orçamento, organização, direção, treinamento e controle das informações. Além da utilidade deveria preocupar-se com suportes tecnológicos voltados ao armazenamento, transmissão, tratamento e conversão de dados, pessoal e financiamento".

No texto *Exploring Information Management*, do professor Andy Bytheway (*South Africa*, 2003), temos uma proposta para início de discussão da Gestão da Informação: "*Information management is the regime that oversees the investment in new information systems and the operation of existing systems. Information management requires the deployment of a diverse range of management skills in order to successfully deliver the benefits of information systems investments*".

Temos ainda o *Business Information Management* (BIM) como sendo "*The process of managing information as a strategic resource for improving organizational performance. This process involves developing strategies and introducing systems and controls to improve information quality to deliver value*" (CHAFFEY, Dave; WOOD, Steve. Business information management. *Improving performance using information systems*. Essex : Harlow, 2005. p.20.).

Vários autores oferecem suas diferentes visões para uma definição do que é a Gestão da Informação, alguns com tendências maiores a negócios, outros ao processamento de dados e informações; alguns poderão ter

visões mais epistemológicas ou voltadas a realidades mais focadas em uma área ou outra. O que nos interessa nesta disciplina GINF-7032 no primeiro semestre de 2019 é a construçaõ do nosso conceito/ definição, bem como um estudo de questões pertinentes tais como estratégia, tecnologia ou riscos – dentre (várias) outras.

2. Valor da Informação

Embora toda organização contenha grande quantidade de informações, as informações naturalmente variam em importância ou valor, em geral classificada conforme o objetivo estratégico. Uma estratégia de gerenciamento de informações obriga uma organização a questionar o valor de suas informações, com a finalidade de atingir um objetivo. A informação pode ser priorizada em importância e em qualidade.

Uma vez que a informação tenha sido identificada como valiosa, podem ser implementadas soluções para:

■ protegê-la de exclusão ou modificação;

■ compartilhá-la dentro de um público definido;

■ melhorar sua qualidade.

Informações de menor valor também podem ser melhoradas para aumentar sua relevância gerencial ou ainda removidas de relatórios detalhados para produzir resumos, uma análise concisa. A entrega de valor ao negócio é a principal razão por trás de uma informação estratégica de gestão, onde agregar valor explorando a informação é um recurso valioso para o negócio, podendo trazer diferenciais que proporcionem tomadas de decisões objetivas para seus negócios, o que pode ser uma forma de se destacar em relação a concorrência que o mercado impõe.

Sugere-se a abordagem de avaliação de risco e valor que envolve a categorização do valor ou importância de diferentes tipos de informação de três maneiras, conforme a tabela abaixo:

Tipo de ativo informação	Valor / importância da informação definida por:		
	Preço pago ou potencialmente pago, custos para obtenção ou manutenção	Impacto de roubo, dano ou perda, grandes erros	Potencial para aumentar a receita ou reduzir custos
1 Informações sobre mercado e clientes			
2 Informação do produto			
3 conhecimento especialista			
4 Informação do processo empresarial			
5 Informações e planos de gerenciamento			
6 Informação sobre recursos humanos			
7 Informações do fornecedor			
8 Informação responsável			

Embora essa tabela seja uma maneira útil de categorizar diferentes tipos de informações, destaca-se que o impacto do roubo ou perda, não é algo muito claro de se identificar e nem muito realista para avaliar tal formação.

Sugere-se que a informação possa ser classificada de acordo com seu valor para a estratégia atual e estratégia futura. Existem quatro categorias:

2.1 Informação Estratégica.

A informação é fundamental para os negócios e é a de maior valor. Isso inclui as informações usadas para gerenciamento de desempenho corporativo, como objetivos, métricas de desempenho e direcionamento do negócio. Também se refere a informações externas, como inteligência competitiva e informação de mercado.

2.2 Informações de Alto Potencial.

O valor potencial para o negócio pode ser alto, mas ainda não está confirmado. A gestão do conhecimento poderia se encaixar nessa categoria de forma a auxiliar as organizações a avaliar se é provável que se tornem informações estratégicas no futuro.

2.3 Informação Operacional Chave.

A informação é essencial para os processos centrais e seu valor é reforçado pela integração horizontal. Este é o maior volume de informações o que envolve transações de vendas, algumas informações de clientes. Tal informação é de valor limitado para estratégia futura, mas relevante para a implementação da estratégia atual.

2.4 Informações de Suporte.

Necessário para apoiar o funcionamento do negócio, mas de pouco valor estratégico. Isso incluiria informações sobre a equipe, como folhas de pagamento, reservas de férias. A gestão desta informação é baixa prioridade, embora ainda necessite ser precisa e econômica.

Tais classificações auxiliam as organizações a avaliar o valor de suas informações, com a finalidade de atingir o objetivo estrategicamente projetado, afim de que seja priorizada a informação e tratada conforme seu valor direto e agregado a estratégia como um todo.

3. Teorias da Informação, Comunicação e Conhecimento: Uma Abordagem Multidisciplinar

Robinson e Bawden são inspirados a responder à questão de John Wheeler: “o que faz sentido?”. O conceito de “informação” em diferentes domínios: tecnológico, físico, biológico, social e filosófico é apontado e comparado. As lacunas entre os vários conceitos de informação nestes 5 domínios são desenvolvidas em mais detalhes. Isso faz com que reconheçam um guia para justificar as diferenças e as lacunas existentes entre eles.

O estilo de escrita utilizado no capítulo oferece recursos mais concretos para cada campo, bem como a história de sua evolução. Além disso, a descontinuidade entre as famílias objetivas / quantitativas / físicas e subjetivas / qualitativas / semânticas dos conceitos de informação é utilizada para identificar e preencher as lacunas.

Os autores estimulam os leitores para que levem em consideração conceitos físicos e biológicos da informação como um conceito vital, ao contrário do que defende Brier. Jonathan Furner descreve cuidadosamente o conceito de “informação sem estudos de informação”.

Ele pretende esclarecer algumas dimensões sobre a natureza das relações entre vários conceitos de informação, como sendo uma coisa única. Ele também tenta desenvolver um framework a fim de definir a gama de possibilidades ontológicas para coisas que foram chamadas de "informações", oferecidas pela ontologia do filósofo Jonathan Lowe (2006).

A ontologia de quatro categorias inclui duas distinções entre substância e objeto: propriedade, tipo, instância e estrutura. Além disso, a distinção entre informação e informatividade pode ser possível, respectivamente, determinando-se como substância ou objeto, e também como propriedade ou modo. Além disso, os conceitos teóricos de probabilidade de informação e informatividade são formulados e elaborados como: surpresa, entropia, entropia condicional e informação mútua.

Como uma profunda sondagem, o conceito de informação sob a perspectiva de Anatoly Rapoport (1955), Tom Stonier (1986) e também Agn`es Lagache (1997), bem como as edições especiais de duas revistas: “informação” e “TripleC” são pesquisadas. Como resultado, Furner, recomenda o uso da ontologia como um meio potencialmente produtivo de identificar possibilidades até então inexploradas. Portanto, ele enfatiza que a informação sem estudos de informação - é empobrecida, por conta do leque de possibilidades ontológicas que ela perde.

4. Qualidade da Informação

Segundo Hassan et al. (2018) a qualidade da informação desempenha um papel significativo na tomada de decisões, além de atender aos requisitos e necessidades de informações dos seus usuários. Também é fundamental na

mitigação de certos riscos. As organizações que não praticam o gerenciamento da qualidade da informação são vistas como "antiéticas" e, portanto, podem ter repercussões em seu desempenho.

5. Segurança da Informação

A informação tem ocupado um papel de destaque nas organizações sendo considerada um ativo, segundo a ISO/IEC 13335-1:2004 ativo é qualquer coisa que tenha valor para a organização. A grande valia da informação nas instituições torna a Segurança de Informação com papel de destaque no ambito organizacional, mantendo a proteção da informação durante todo seu ciclo, abrangendo: sistemas, aplicativos, equipamentos, serviços e pessoas.

Segundo US National Security Telecommunications and Information Security Committee a segurança da informação é definida “como proteção das informações e dos sistemas e equipamentos que utilizam, armazenam e transmitem essas informações”.

A NBR ISO/IEC 27002:2005 define a segurança da informação como a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio.

Sêmola (2003) define segurança da informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.”

5.1.1 Classificação

Segundo Sêmola (2003), a gestão da segurança da informação pode ser classificada em três aspectos: tecnológicos, físicos e humanos. As organizações preocupam-se principalmente com os aspectos tecnológicos (redes, computadores, vírus, hackers, internet) e se esquecem dos outros – físicos e humanos – tão importantes e relevantes para a segurança do negócio quanto os aspectos tecnológicos.

A camada física refere-se onde está instalado fisicamente o hardware, servidores, computadores podendo ser na empresa, fábrica, em casa (por acesso remoto), algumas formas de proteção a essa camada seria controle

de acesso a recursos de TI, fornecimento inenterrupto de energia e firewalls.

A camada lógica abrange uso de softwares responsáveis pela funcionalidade do hardware, transações de bases de dados, criptografia de senhas, para Netto apud Adachi(2004) é nessa camada que estão as "regras, normas e protocolos de comunicação", mantendo os softwares somente atualizados com a mais recente correção de segurança disponibilizada pelo fabricante minimiza os riscos de segurança nessa camada.

Na camada humana formada pelos recursos humanos, há percepção dos riscos pelas pessoas: como elas lidam com os incidentes de segurança que ocorrem. A politica de segurança e a conscientização dos usuários são algumas das formas de se controlar a segurança desta camada.

As principais caracteristicas da segurança de informação são:

- Disponibilidade. Garantir que as informações estejam disponíveis para aqueles que precisam delas e que elas possam usá-las quando apropriado.
- Confidencialidade. Garantir que o acesso às informações esteja disponível apenas para aqueles que precisam delas. O lado oposto ao da disponibilidade.
- Autenticidade e integridade. Garantir que a informação é oriunda da fonte que lhe é atribuída e elaborada e garantir que toda a informação não foi corrompida e nem alterada garantindo a precisão das informações.

5.1.2 Politica de Segurança

De acordo com Chaffey e Wood(2005), sabe-se que as informações devem ser protegidas contra modificações acidentais, eventos naturais, modificações intencionais. Para isso muitas organizações implementam politicas de segurança para proteger os ativos de informação. A politica de informação pode ser tanto desenvolvida pela própria organização como também adotada por politicas já existentes, um exemplo seria a norma BS7799 (Standards: British Standard for Information Security) essa norma define dez principios orientadores para politica de segurança de informação que são:

- Política de segurança
- Organização da segurança
- Classificação e controle de ativos
- Segurança do pessoal
- Segurança física e ambiental
- Gestão da comunicação e das operações
- Controle de acesso
- Desenvolvimento e manutenção de sistemas
- Planejamento da continuidade do negócio
- Conformidade.

5.1.3 Análise de Segurança

Exige uma avaliação dos seguintes domínios:

- Ativos de informação - quais são os principais recursos que estamos tentando proteger? O que eles valem? Que nível de segurança podem ser atribuídos?
- Avaliação de ameaças - uma lista comum de ameaças à segurança da informação incluiria: - Erros humanos: atos inadvertidos, que podem ser internamente por funcionários ou externamente por provedores de serviços - Falha de sistema: uma falha técnica de software ou hardware - Desastres naturais: incêndio, inundação, etc. – Ações maliciosos: deliberados de sabotagem.
- Avaliação de impacto - quais são as implicações de nossos ativos de informação serem comprometidos? Os impactos podem incluir: - Interrupção do sistema - Violação da confidencialidade da informação - Destruição ou corrupção da informação.
- Avaliação de falhas de segurança - de que forma nossos sistemas podem ser comprometidos, como por exemplo: - Falhas de projeto - Engenharia social (obtenção de informações de segurança por engano). As evidências dessa análise levarão ao desenvolvimento de controles para garantir que os objetivos de segurança sejam atingidos.

5.2 Gestão da Segurança da Informação: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas

De acordo com um estudo exploratório realizado por Netto (2007) com o objetivo de identificar em que medida as pequenas e médias empresas

adotam a segurança da informação. Com uma amostra de 43 industrias do setor de produtos de metal, classificando a segurança de informação em camada física, lógica e humana. Identificou que a camada humana é a que apresenta maior carência de cuidados por parte das empresas. Seguida pela camada lógica. O antivirus é a ferramenta mais utilizada pelas empresas pesquisadas, e o principal motivador para adoção de gestão da segurança da informação é “evitar possiveis perdas financeiras”.

Diante das diversas maneiras de perdas da informação como: spyware, botnets, virus, warms, até mesmo pessoas da própria empresa ou externas acessarem as informações valiosas das empresas. Quanto custa a perda ou a falta de confiabilidade nas informações? A resposta a esta questão motiva a criação de um novo assunto para o capítulo a seguir: de que maneira são gerenciados os riscos numa organização, qual é melhor maneira de evitá-los, e onde a segurança de informação se encaixa no gerenciamento de riscos.

6 Ética e Regulamentação Legal

Uma vasta informação, requer um maior número de leis regulamentares, obrigando os governos a desenvolver mais e mais leis nesse sentido. No entanto a lei pode ser violada, a exemplo de:

- Compartilhar dados do cliente sem o seu consentimento,
- Enviar e-mails não solicitados,
- E-mail entre funcionários denegrindo a imagem alheia,
- Monitorar acesso de funcionários à dados,
- Não prover acesso visual para deficientes.

Em cada fase do ciclo da informação, devem ser adotadas medidas visando o *Legal Compliance* dos dados.

As fases do ciclo de vida da informação são:

- Capturar,
- Organizar,
- Processar,
- Manter,
- Destruir.

De acordo com o British Standards Institute (BSI, 2001) um registro é identificado como sendo uma informação criada, recebida e mantida, como evidência e informação sobre uma organização ou pessoa, devido às obrigações legais, ou na transação de negócios.

Com relação à gestão dos registros, estes seguem 3 estágios:

- Na criação e captura de registros, o tempo e local da criação de novos dados do cliente devem ser armazenados de forma transparente para uma eventual reclamação.
- O acesso aos registros e sua modificação também deve ser armazenado.
- Ao eliminar um registro este deve obedecer a política estabelecida na empresa, que deve prever quanto tempo o registro deve ficar armazenado, porém podem existir questões legais de tempo de armazenamento de registros, essas também devem ser respeitadas.

Devido a alguns escândalos contábeis, a necessidade pela acuracidade da informação aumentou drasticamente, levando o governo do Estados Unidos a introduzir o Ato Sarbanes-Oxley em 2002, requerendo um controle rígido sobre a exatidão dos dados financeiros, o CIO – Chief Information Officer deve assinar um documento que confirma que o sistema de tecnologia da informação existente na corporação suporta a integridade financeira dos dados e que são confirmados pelo responsável financeiro. Práticas semelhantes vêm sendo adotadas em outros países.

Algumas restrições de compliance que não ferem a lei, no entanto são eticamente controversas, como o envio de e-mails não solicitados. Estas devem ser observadas e contornadas através de, por exemplo, um termo de consentimento.

6.1 Por que Profissionais em Privacidade de Dados Precisam de uma Nova Abordagem ao Compliance

Temos visto organizações governamentais criando leis para acesso de dados individuais, como no Brasil, a Lei Geral de Proteção de Dados Pessoais, na California a *Consumer Privay Act* e no Vietnam a *Cybersecurity law*.

Existem requisitos comuns que abrangem muitas dessas leis de

privacidade ou regulamentos de proteção de dados.

6.1.1 Inventário de Dados e Mapeamento

As leis de informação esperam que sua organização saiba porque dados pessoais estão sendo coletados, o que é feito com eles, quais os dados coletados e quais tecnologias estão processando dados pessoais.

Para algumas organizações essa tarefa pode parecer assustadora, devendo ser dividida em duas abordagens distintas: manual e automatizada.

6.1.2 Abordagem Manual

Requer uma quantidade de tempo para verificar e validar os dados.

6.1.3 Abordagem Automatizada

Usa descoberta de dados e ferramentas de scan para desenvolver inventário de dados e mapeamento, essa abordagem dispende menor esforço, porém deve ser verificada se a tecnologia utilizada está alinhada com a política e ambiente de TI da empresa.

6.1.4 Retenção e Descarte

Muitas organizações já implementaram uma política de retenção por tempo e descarte dos dados, no entanto muitas organizações possuem dificuldade nessas áreas, porém essas são críticas ao sucesso da área de gestão da informação.

6.1.5 PIA/DPIA

Na maioria das vezes a identificação e avaliação dos riscos é feito sob a perspectiva da organização, no entanto o PIA/DPIA foca no titular dos dados.

Toda organização deve ter sua abordagem, mas as leis têm transformado como as organizações atuam.

7. Ética na Computação

A disponibilidade de software de alta qualidade é crítica para o uso efetivo de TI em organizações. Embora o uso desse tipo de software seja fundamental, sua utilização é cercada por problemas, parte deles por falta de avaliação de riscos. Neste contexto entra a análise de risco expandida, que visa mitigar a maioria destes erros. É apresentada também uma ferramenta chamada SoDIS – Software Development Impact Statement, ou seja, uma declaração de impacto no desenvolvimento de software.

Alguns exemplos de riscos no desenvolvimento de software incluem prazos extrapolados, sobre-preço, falha em atender o objetivo do cliente e principalmente, falhas de segurança. Padrões genéricos foram desenvolvidos no sentido de criar padrões em um modelo de análise de risco:

- *Context* - (o contexto) representa o contexto em que um projeto é desenvolvido, evidenciando os elementos contextuais que podem interferir no sucesso do projeto.
- *Risk Identification* - O processo de identificação de riscos identifica potencial impacto negativo sobre o projeto e seus stakeholders. AS/ NZS lista potenciais áreas negativas de impacto, como ativo e base de recursos da organização, receita e direitos, custos, desempenho, tempo, cronograma de atividades e comportamento organizacional (AS / NZS, 1999, p. 39).
- *Risk Analysis* – Análise de risco, uma vez que esses efeitos potenciais de risco tenham sido identificados, eles são priorizados na fase de análise de risco para ajudar a ordenar quando e se eles serão abordados. Os riscos são classificados em altos, moderados e baixos. Também são feitas análises quantitativas e qualitativas de riscos. A análise qualitativa se classifica em 1-insignificante, 2-pequeno, 3-moderado, 4-alto e 5-catastrófico.

As limitações dos “padrões genéricos” - A *Association for Information Systems* define “qualidade do sistema” em termos de moeda, tempo de resposta, tempo de retorno, precisão dos dados, confiabilidade, integridade, flexibilidade do sistema e facilidade de uso (AIS, 2005). Porém esses padrões não tratam de impactos sociais e éticos. Para Hilson (2004), os principais estágios da análise de risco ao longo de um ciclo de vida de software consistem na especificação e teste de requisitos de

segurança do sistema:

- Riscos Éticos - As partes éticas interessadas no software desenvolvido são todas aquelas que são afetadas por ele, mesmo que não estejam diretamente relacionadas ao uso ou financiamento de um sistema, como por exemplo, alguém que teve sua identidade invadida, através de um sistema.
- *Software Development Impact Statement* (SoDIS) - como uma declaração de impacto ambiental, é usada para identificar potenciais impactos negativos de um sistema proposto e especificar ações que mediarão esses impactos. O SoDIS tem como objetivo avaliar os impactos decorrentes tanto do processo de desenvolvimento de software quanto das obrigações mais gerais para os diversos interessados.
- Identificação dos *Stakeholders* - Uma identificação preliminar das partes interessadas do projeto de software é realizada examinando o plano e as metas do sistema para ver quem é afetado e como eles podem ser afetados.

Em um alto nível, o processo SoDIS pode ser reduzido a quatro etapas básicas: (1) a identificação das partes interessadas imediatas e estendidas em um projeto, (2) a identificação das tarefas ou pacotes de divisão de trabalho em um projeto, (3) para cada tarefa, a identificação e registro de potenciais questões éticas violadas pela conclusão dessa tarefa para cada parte interessada, e (4) o registro dos detalhes e soluções de questões éticas significativas que podem estar relacionadas a tarefas individuais e um exame de se a tarefa atual precisa ser modificada ou uma nova tarefa criada para resolver a preocupação identificada.

Identificação de *Stakeholders* SoDIS - A identificação das partes interessadas deve encontrar um equilíbrio entre uma lista de partes interessadas que inclua pessoas ou comunidades que sejam eticamente remotas em relação ao projeto e uma lista de partes interessadas que inclua apenas uma pequena parcela das partes interessadas eticamente relevantes. O SoDIS fornece uma lista padrão de partes interessadas relacionadas à maioria dos projetos.

Identificação de Tarefas ou Requisitos - Em cada estágio do desenvolvimento do sistema, há uma série de tarefas ou requisitos que decompõem o desenvolvimento em suas partes componentes. Essas descrições de tarefas individuais são usadas na revisão e monitoramento do

projeto. Cada uma dessas tarefas individuais pode ter um impacto ético significativo.

Identificando possíveis problemas éticos - Este processo de identificação das partes interessadas foi modificado no Auditor do Projeto SoDIS. Os princípios éticos de Gert foram combinados com imperativos éticos de vários códigos de ética da computação para refletir a responsabilidade profissional positiva dos desenvolvedores de software.

Melhore a auditoria SoDIS com um modelo de inspeção - Os resultados de pesquisas anteriores sobre projetos fracassados e nosso uso inicial da análise SoDIS (Gotterbarn e Rogerson, 2005) levaram os autores do projeto a fazer modificações significativas na forma genérica de análise de risco.

O sodis e os requisitos de voto eletrônico do Reino Unido - O modelo de inspeção do SoDIS (ver seção 18.3) foi desenvolvido em parte por meio do trabalho com o governo do Reino Unido.

7.1 GlaxoSmithKline

A Fusão de duas grandes companhias oferece inúmeros desafios do ponto de vista de gestão e do gerenciamento da informação.

Foram criadas políticas para retenção de registros, privacidade de dados, classificação e proteção da informação e *Copyright*.

O grupo global de gerenciamento de documentos empreendeu um treinamento nas melhores práticas do gerenciamento da informação.

Políticas empresariais são necessárias mas o gerenciamento da informação e práticas com documentos como armazenamento e cuidados adicionais precisam vir das pessoas da equipe, conscientização que pode ser conseguida através do treinamento.

7.2 As Crescentes Implicações Legais e Reguladoras da Coleta de Dados Biométricos

Nos últimos anos, as tecnologias biométricas de impressão digital para reconhecimento facial estão sendo cada vez mais utilizadas pelos

consumidores para uma ampla gama de casos de uso, que vão desde pagamentos para bagagem de mão no aeroporto e até mesmo a bordo de um avião. Embora essas tecnologias geralmente simplifiquem a experiência de autenticação do usuário, elas também introduzem novos desafios de privacidade em torno da coleta e armazenamento de dados biométricos.

Nos EUA, os reguladores estaduais reagiram a essas preocupações crescentes em torno de dados biométricos ao promulgar ou propor legislação. Illinois foi o primeiro estado a promulgar tal lei em 2008, o Biometric Information Privacy Act (BIPA). O BIPA regula como organizações privadas podem coletar, usar e armazenar dados biométricos. O BIPA também permitiu que indivíduos processassem organizações individuais por danos com base no uso indevido de dados biométricos.

Embora tenha uma década, o BIPA ganhou recente destaque devido à decisão de janeiro de 2019 do Supremo Tribunal de Illinois, Rosenbach vs. Six Flags. Neste caso, os pais de um menor processaram o parque de diversões Six Flags Great America em Gurnell, Illinois, argumentando que os dados biométricos foram coletados sem o consentimento e violaram o BIPA.

De um modo geral, os parques de diversões têm exigido cada vez mais que os indivíduos digitalizem seus ingressos, seguidos por um escaneamento biométrico em uma catraca. Esse processo é basicamente uma medida antifraude: se você perder seu ticket/passe, forneça seus dados biométricos em um balcão de atendimento ao cliente para obter um novo. Este processo reduz os fraudadores de tentar obter um passe livre alegando que perderam seu ticket.

A Suprema Corte de Illinois reverteu as decisões do tribunal de primeira instância e decidiu que o Six Flags havia violado o BIPA. É importante ressaltar que a Suprema Corte de Illinois determinou que os queixosos não tinham que comprovar os danos recebidos (como roubo de identidade) pela coleta de dados biométricos. A coleta inadequada de dados biométricos foi suficiente para permitir que consumidores individuais processassem organizações no âmbito do BIPA.

Essa decisão é uma vitória para os direitos do consumidor e da privacidade e levará a mais desafios legais ao BIPA, muitos dos quais já estão em progresso no sistema judicial. Um caso a ser monitorado é o Patel vs.

Facebook, que está atualmente em análise no *Ninth Circuit Court of Appeals*, em San Francisco, e envolve desafios contra a marcação no Facebook de imagens faciais carregadas do Facebook.

Massachusetts, Nova York e Michigan têm contas de privacidade em desenvolvimento que possuem requisitos semelhantes ao BIPA, e mais estados provavelmente considerarão a elaboração de leis que regem a coleta, o uso e o armazenamento de dados biométricos.

Esses desenvolvimentos não significam a sentença de morte da biometria. Eles apenas indicam que as organizações que estão considerando coletar dados biométricos devem aderir às abordagens de privacidade por design e fornecer requisitos adequados de divulgação, consentimento e desativação, bem como prestar atenção a esse ambiente legislativo cada vez mais complexo para garantir que a coleta de dados biométricos e a retenção está sendo feita de acordo com essas leis emergentes.

8. Gestão do conhecimento e gestão da informação.

8.1. Dados, Informação e Conhecimento

O objetivo deste capítulo é entender os conceitos de dados, informação e conhecimento e os fatores envolvidos na transformação de dados em informação, e informação em conhecimento.

Dados caracterizam-se por simples observações sobre o estado do mundo, e sua observação pode ser feita por pessoas ou tecnologia apropriada. Dados são facilmente estruturados, quantificados e transferíveis, sendo a matéria-prima essencial para a criação de informação.

A partir de um conjunto de dados, a informação é originada e explicitada como mensagem, contextualizada, categorizada, calculada, corrigida e/ou condensada. A informação consiste em dados de relevância e propósito, e requer consenso em relação ao significado.

O conhecimento pode ser visto como uma mistura fluida de experiência condensada, valores, informações contextuais e percepções especializadas, a qual proporciona uma estrutura para avaliar e incorporar novas

experiências e informações. O conhecimento tem origem e é aplicado a mente dos conhecedores.

O conhecimento inclui reflexão, síntese e contexto, sendo de difícil estruturação, captura e transferência.

A transformação de informação em conhecimento ocorre através de processos humanos, como comparações e conversações.

8.2.1 Conceitos de Dados x Informação x Conhecimento

Drucker (2000) estabelece uma relação entre os termos “dado”, “informação” e conhecimento, discorrendo que informação pode ser entendida como dado incrementado de propósito e relevância, todavia, para transformar dado em informação é necessário que se tenha conhecimento.

8.2.2 Conceitos de Dado

1) Laudon e Laudon (2004, p. 7) conceituam dado como sendo: [...] correntes de fatos brutos que representam eventos que estão ocorrendo nas organizações ou no ambiente físico, antes de terem sido organizados e arranjados de uma forma que as pessoas possam entendê-los e usá-los.

2) “Dado: elemento que representa eventos ocorridos na empresa ou circunstâncias físicas, antes que tenham sido organizados ou arranjados de maneira que as pessoas possam entender e usar.”

3) Davenport e Prusak (1998, p. 2) descrevem dados como “um conjunto de fatos distintos e objetivos, relativos a eventos e que, em um contexto organizacional, são descritos como registros estruturados de transações”.

8.2.3 Conceitos de Informação

1) “Informação: Dado configurado de forma adequada ao entendimento e à utilização pelo ser humano.”

2) Informação é o dado trabalhado que permite ao executivo tomar decisões (Oliveira, 2005)

3) Informação não é Conhecimento, informação é diferente de Conhecimento. A informação (matéria-prima para o conhecimento) é um bem comum ao qual todo cidadão deve ter direito/acesso, levando à socialização da informação, das oportunidades e do poder (Rezende, 2014).

8.2.4 Conceitos de Conhecimento

1) Para Pimenta (2008), o conhecimento pode ser compreendido como o resultado da interpretação da informação e de sua utilização para alguma finalidade.

2) Capurro e Hjorland (2007) consideram que o termo informação costuma ser utilizado geralmente para designar uma ação, forma de moldar a mente ou o ato de comunicar, transmitir conhecimento. A informação para uma organização deve ser constituída como um conjunto de dados selecionados, analisados e disponibilizados e com valor agregado. É o componente fundamental para a realização de qualquer tipo de tarefa.

3) Conhecimento é uma informação contextual, relevante e acionável. Dito de forma simples, conhecimento é a informação em ação. Capital intelectual (ou recursos intelectuais) é outro termo frequentemente usado como sinônimo de conhecimento (TURBAN; Rainer Jr; Kelly; Potter, 2007).

4) Para DAVENPORT e PRUSAK (1998) o conhecimento pode ser visto como uma mistura fluida e experiência condensada, valores, informação contextuais e insight experimentado, a qual proporciona uma estrutura para a avaliação e incorporação de novas experiências e informações. O conhecimento tem origem e é aplicado a mente dos conhecedores.

8.3 Gestão do Conhecimento e o Perfil do Trabalhador

Negócios e processos fundamentados em conhecimento, globalização, internet, comunicação, competitividade, impulsionados pelas crises econômicas e as constantes inovações tecnológicas. Tudo isso tem exigido um perfil de trabalhador diferenciado, onde o conhecimento é parte integrante da formação e atuação do mesmo. Competências e Habilidades como abstração, inovação, solução de problemas, negociação são fundamentais neste cenário. Como este profissional está lindando frente a

isso com a gestão do conhecimento? Como trabalhar os mesmos em uma matriz de responsabilidades visando o melhor cenário?

Neste contexto é interessante observar o perfil do trabalhador baseado em conhecimento, atividade e execução (ação e reação). Sua relação com esse processo determina como o trabalhador está perante essas novas competências e habilidades exigidas por este mercado. Qual o perfil do trabalhador deste novo contexto, desta nova economia (designs novos, equipes ágeis e multifuncionais, comunicação multilaterais, informações compartilhadas em redes e comunidades).

Para Reinhard *et al.* (2011), o objeto do conhecimento é produzido pelo trabalhador mediante a sua capacidade racional durante o processo de trabalho e por sua interação com os indivíduos e o ambiente.

Conforme MACEDO, SANTOS, JOÃO, e SAITO (2016, p. 97), para identificar quais as atividades relacionadas ao papel do trabalhador do conhecimento (Quadro 1), Reinhardt *et al.* (2011) teve como base o estudo de Hädrich (2008); ao definir que "*knowledge work is characterized by certain knowledge actions and different roles that knowledge workers take on*".

Quadro 1: Tipologia de papéis e características das atividades dos trabalhadores do conhecimento na visão de Reinhardt *et al.* (2011)

Papéis	Atividades	Autores
1. Controlador	Monitora o desempenho da organização baseado em informações de várias fontes.	Moore e Rugullies (2005) Geisler (2007)
2. Auxiliar	Transfere informações para ensinar os colegas que passaram por problemas recentemente.	Davenport e Prusak (1998)
3. Aprendiz	Utiliza a informação e as práticas para a melhoria das suas habilidades e competências pessoais	Reinhardt et al. (2011)
4. Linker	Associa e combina informações de diferentes recursos para gerar novas informações.	Davenport e Prusak (1998) Nonaka e Takeushi (1995) Moore e Rugullies (2005)
5. Networker	Constrói relações pessoais e/ou profissionais com pessoas envolvidas no mesmo perfil de trabalho, compartilhando informações e oferecendo apoio a sua rede.	Davenport e Prusak (1998) Nonaka e Takeushi (1995) Moore e Rugullies (2005)
6. Organizador	Planeja atividades pessoais e da organização, por exemplo, lista de tarefas.	Moore e Rugullies (2005)
7. Recuperador	Pesquisa e coleta informações sobre um determinado tópico.	Snyder-Halpern et al. (2001)
8. Compartilhador	Divulga informações em comunidades.	Davenport e Prusak (1998) Brown et al. (2002) Geisler (2007)
9. Solucionador	Identifica ou fornece opções para a resolução de um problema.	Nonaka e Takeushi (1995) Moore e Rugullies (2005)
10. Rastreador	Monitora e reage com ações pessoais e	Moore e Rugullies (2005)

Fonte: Adaptado de Reinhardt *et al.* (2011) por MACEDO, SANTOS, JOÃO, e SAITO (2016, p. 97 e 98)

Para Reinhardt *et al.* (2011) as tarefas em organizações voltadas ao conhecimento intensivo resistem à padronização de atividades por causa de sua natureza contingencial. Ao definir 13 processos típicos do conhecimento (Quadro 2) esperado leva-se em consideração as ações que os trabalhadores do conhecimento realizam durantes as suas tarefas:

Quadro 2: 13 Processos Típicos do Conhecimento do Trabalhador na visão de Reinhardt *et al.* (2011)

1.Aquisição: buscar conhecimento, nos meios de informação, com o objetivo de desenvolver habilidades, estruturar um projeto ou obter um objeto.
2. Análise: examinar ou pensar, cuidadosamente, para compreender algo.
3. Busca de informação: procurar informações sobre tópicos específicos de uma forma específica, utilizando sempre uma estrutura de pastas em um sistema ou um sistema de recuperação da informação
4. Busca de informação especializada: recorrer a um especialista para discutir e encontrar soluções para um problema específico.
5. Organização de informação: organizar informações pessoais e organizacionais.
6. Monitoração: manter organizado e/ou atualizado tópicos selecionados, por exemplo, com base em diferentes tecnologias de informação.
7. Autoria: criar um texto e/ou uma mídia utilizando um software ou um sistema de processamento de texto ou apresentação.
8. Coautoria: colaborar na criação de um texto e/ou uma mídia utilizando um software ou um sistema de processamento de texto ou apresentação.
9. Disseminação: compartilhar informações ou objetos/conteúdos, sempre sobre resultados obtidos no trabalho.
10. Aprendizagem formal e informal: adquirir novo conhecimento, habilidade ou compreensão durante a execução de uma atividade ou baseado em conteúdo (material) da aprendizagem formal.
11. Feedback: avaliar uma proposta ou o conteúdo da informação.
12. Networking: interagir com outras pessoas e organizações para troca de informações e desenvolvimento de relacionamentos.
13. Busca de serviços: identificar serviços especializados através da Web, por exemplo, serviço de tradução.

Fonte: Adaptado de Reinhardt *et al.* (2011) por MACEDO, SANTOS,

JOÃO, e SAITO (2016, p. 98)

Conforme MACEDO, SANTOS, JOÃO, e SAITO (2016, p. 106) o uso da tipologia do trabalhador do conhecimento pode colaborar a identificar os colaboradores e adequar seus perfis aos papéis e, assim ajudar na melhoria da gestão de recursos, de processos e na sua alocação voltado a gestão do conhecimento.

8.4 Diferenças entre Gestão do Conhecimento e Gestão da Informação

Para identificar essa diferença, surgem técnicas adquiridas através da Gestão de Conhecimento e da Gestão da Informação. De acordo com Valentim (2004), Gestão de Informação é um conjunto de estratégias que visam identificar as necessidades informacionais, mapear os fluxos formais de informação nos diferentes ambientes da organização. Por outro lado, a Gestão do Conhecimento é o conjunto de estratégias para criar, adquirir, compartilhar e utiliza alvos de conhecimento, bem como estabelece fluxos que garantam a informação necessária no tempo e formato adequados, a fim de auxiliar na geração de ideia. Além disso, existem algumas vertentes que fundem os dois modelos de gestão. Ambos modelos focam para o fato de que pretendem apoiar as atividades desenvolvidas no dia a dia e na tomada de decisão, mas focam em fluxos informacionais diferenciados, sendo a Gestão de Informação nos fluxos formais (conhecimento explícito – do latim *explicitus* , quando o conhecimento está declarado, mostrado, explicado) e a Gestão de Conhecimento nos fluxos informais (conhecimento tácito – do latim *tacitus*, quando o conhecimento não pode ser exteriorizado por palavras; como: construção individual de conhecimento, valores, crenças e comportamento organizacional).

Os sistemas de informação buscam pela tradução do conhecimento tácito, como afirma GIL (1999) explicando que eles devem compreender um conjunto de recursos humanos, materiais, tecnológicos e financeiros agregados segundo uma sequência lógica para o processamento dos dados e a correspondente tradução em informações. Traduzindo-se em Sistema de Informação Gerencial (SIG), ele é projetado para oferecer aos administradores informações seguras para a tomada de decisão, sendo esse o ponto de interesse do estudo da informática nas organizações. “Um Sistema de Informações Gerencial (SIG) abrange uma coleção organizada

de pessoas, procedimentos, software , banco de dados e dispositivos que fornecem informação rotineira aos gerentes e aos tomadores de decisão. O foco de um SIG é, principalmente, a eficiência operacional. Marketing , produção, finanças e outras áreas funcionais recebem suporte dos sistemas de informação gerencial e estão ligados através de um banco de dados comum" (STAIR & REYNOLDS, 2002, p. 18).

Percebe-se através das definições que um SIG nada mais é que ferramentas que auxiliem e permitam aos gestores de forma dinâmica e prática embasar as informações necessárias para as decisões que norteiam as empresas. As tomadas de decisões envolvem um ciclo e é fundamental a existência de informações apropriadas a cada uma das fases do ciclo sendo elas de implantação, avaliação da decisão, recomendações de mudanças e tomada de decisão. Cabe aos analistas e desenvolvedores de tais sistemas adaptá-los e implementá-los quanto aos pontos inerentes ao cenário analisado. Essa área de estratégia empresarial é conhecida como *Business Intelligence*, ou Negócio Inteligente, que tem por finalidade auxiliar as organizações por meio da automatização dos processos empresariais.

9 Suporte Tecnológico

O suporte da TI desempenha um papel crítico nos esforços de gerenciamento de conhecimento e de informação entre as empresas.
Fornecer o suporte tecnológico adequado para o mapeamento correto do processo e sua modelagem auxiliará na estratégia de gerenciamento de informações. Os recursos de infraestrutura de tecnologia são as redes de hardware e software usadas para armazenar, processar e transmitir as informações em uma organização.

Na opinião de Gómez (2017), o progresso constante nos sistemas e tecnologias da informação e comunicação afeta todos os ambientes empresariais. Não só aqueles onde a tecnologia é a base do desempenho da empresa, mas também nas empresas que utilizam essas ferramentas em sua organização interna, fazendo parte de seus produtos ou serviços, ou mesmo onde a informática é um elemento essencial para entrar em contato e comunicar-se com os clientes.

9.1 *Data Warehouse*

Data Warehouse (DW) é o nome dado ao repositório de dados históricos, relacional ou multidimensional, que serve aos interesses de todos os departamentos da organização (BARBIERI, 2011; BATISTA, 2012). Um DW se diferencia de um banco transacional principalmente pela não volatilidade (dados não podem ser modificados pelo usuário), pelo tempo que ficam armazenados, pois não são excluídos dados com o passar do tempo e pela forma de armazenamento dos dados por assunto, sumarizados no tempo (BARBIERI, 2011; BATISTA et al., 2012).

De acordo com Machado (2000), o DW é um sistema de computação utilizado para armazenar informações relativas às atividades de uma organização em bancos de dados, de forma consolidada. São as chamadas séries históricas que possibilitam uma melhor análise de eventos passados, oferecendo suporte às tomadas de decisões presentes e à previsão de eventos futuros.

Data Warehouse é um processo que aglutina dados de fontes heterogêneas, incluindo dados históricos e dados externos para atender a necessidade de consultas estruturadas e ad hoc, relatórios analíticos e de suporte a decisão (HARJINDER, RAO, 96)

O DW não é um produto que possa ser comprado como um software de banco de dados; nem aprendido ou codificado como uma linguagem; nem é somente um modelo de banco de dados ou a constituição de vários modelos. O sistema de data warehouse deve ser pensado como um processo que está sempre em crescimento para disponibilizar informações que apoiem as decisões estratégicas da organização.

Um *data warehouse* concentra dados de diversos sistemas estruturados e outras bases de dados, em diferentes plataformas. Os dados antes de serem armazenados são filtrados, normalizados, reorganizados, sumarizados para constituírem uma base de dados confiável e íntegra.

O principal objetivo de um DW é de fornecer os subsídios necessários para a transformação de uma base de dados uma organização, geralmente transacionais, online e operacional denominado banco de dados OLTP (*Online Transation Processing*), para uma base de dados maior que contenha o histórico de todos os dados de interesse existentes na

organização, denominado de banco de dados OLAP (*Online Analytical Processing*).

9.2 *Business Intelligence*

Um sistema automático para disseminar informação para vários setores de qualquer empresa, utilizando máquinas de processamento de dados (computadores), auto-abstração e auto-codificação de documentos e criando perfis para cada ponto de ação da organização por palavra padrão (LUHN, 1958).

"... É um termo guarda-chuva que inclui as aplicações, infraestrutura e ferramentas e as melhores práticas que permitem acesso e análise de informações para promover e otimizar decisões e performance" (GARTNER, 2013).

"... refere-se à coleção de SIs e de tecnologias que dão suporte à tomada de decisão gerencial ou operacional – controle pelo fornecimento de informações nas operações internas e externas" (TURBAN & VOLONIMO, 2013)

"... refere-se às aplicações e tecnologias que são utilizadas para coletar, acessar e analisar dados e informações de apoio à tomada de decisão" (BALTZAN & PHILLIPS, 2012).

"... É o processo de transformação de dados brutos em informações utilizáveis para maior efetividade estratégica, insights operacionais e benefícios reais para o processo de tomada de decisão nos negócios" ((DUAN & XU, 2012).

As ferramentas de BI podem fornecer uma visão sistêmica do negócio, sendo seu objetivo principal transformar grandes quantidades de dados em informações de qualidade para a tomada de decisões. Através delas, é possível cruzar dados, visualizar informações em várias dimensões e analisar os principais indicadores de desempenho empresarial. (Batista, 2004).

O conceito de *Business Intelligence* com o entendimento de que é Inteligência de Negócios ou Inteligência Empresarial compõe-se de um conjunto de metodologias de gestão implementadas através de ferramentas de software, cuja função é proporcionar ganhos nos processos decisórios

gerenciais e da alta administração nas organizações, baseada na capacidade analítica das ferramentas que integram em um só lugar todas as informações necessárias ao processo decisório. Reforça-se que o objetivo do *Business Intelligence* é transformar dados em conhecimento, que suporta o processo decisório com o objetivo de gerar vantagens competitivas (ANGELONI E REIS, 2006).

"..um guarda-chuva conceitual, visto que se dedica à captura de dados, informações e conhecimentos que permitam às empresas competirem com maior eficiência em uma abordagem evolutiva de modelagem de dados, capazes de promover a estruturação de informações em depósitos retrospectivos e históricos, permitindo sua modelagem por ferramentas analíticas. Seu conceito é abrangente e envolve todos os recursos necessários para o processamento e disponibilização da informação ao usuário" (ANGELONI E REIS, 2006)

Os componentes da ferramenta de BI consistem na extração, transformação e cargas dos dados (ETL), no armazenamento dos dados (DW) e Data Marts, na análise de informações (OLAP) e na mineração de dados (DM).

10 Função do Gerenciamento da Informação

Além da criação de uma responsabilidade geral pela informação na organização como um todo, sugere-se que tais responsabilidades devam ser definidas em todas as partes da empresa. Citando Evernden& Evernden (2003), os autores definem 4 tipos de responsabilidade em relação às informações:

1 - Governança - Gerentes responsáveis pela direção global e pelo (controle do) gerenciamento de informações, o que envolve a obtenção de financiamento para projetos e sistemas que visem melhorar a qualidade da informação e a liderança de sua implementação.

2 - Administração - a administração da informação envolve a qualidade da informação e é responsável por atividades tais como criação ou captura, disseminação e apagamento.

3 - Infraestrutura - criação do ambiente correto para uso da informação, o que envolve estabelecer e integrar sistemas e bancos de dados, criação de

bancos de dados e arquiteturas informacionais para páginas web e a proteção dos recursos de informação.

4 - Uso - trata-se da responsabilidade que o usuário final tem pela informação, o que envolve o uso em si e atividades que incluem avaliar a apontar problemas com sua qualidade.

Os autores frisam que tal lista faz com que todos em uma organização sejam reponsáveis por suas informações. Após breve exemplo citam *guidelines* para o desenvolvimento de uma estratégia informacional que passam pelo estabelecimento de um comitê, um gerente/ diretor, guardiães das informações (manutenção de padrões, auditoria, delegação de responsabilidades), usuários e um serviço de informações. Com isto, introduzem a figura do CIO, *Chief Information Officer*, um gestor com a responsabilidade pelos ativos de informação e/ ou pela estratégia dos sistemas de informação.

11 Gerenciamento do Risco da Informação

11.1 Gerenciamento do Risco da Informação (Information Risk Management – IRM)

Conjunto de políticas, procedimentos, processos e tecnologia adotados para reduzir as ameaças e vulnerabilidades que possam vir a ocorrer caso dados não sejam protegidos.

11.2 Podemos ter Ameaças Intencionais e não Intencionais

A ameaça intencional envolve intenção direta de roubar os dados da empresa, essa ação pode ser exemplificada pelo ataque de um hacker, enquanto que a ameaça não intencional se refere ao vazamento de informações devido a um descuido, por exemplo quando um funcionário deixa documentos sigilosos à mostra fora da empresa ou quando um gestor de TI não é tão cuidadoso com a infraestrutura e segurança.

11.3 Entendendo a Equação do Risco

A equação do risco é formada por três variáveis:

- **Ameaça**

Pode ser associada à taxa de frequência, por exemplo: A taxa de furacões na Flórida é de 1.4 por ano.

Pode ser categorizada em taxas de ameaça global e taxa de ameaça local, como áreas geográficas, situação política, entre outros indicadores.

É fundamental determinar, ou ao menos estimar, cada ameaça que possa afetar a organização.

- **Vulnerabilidade**

È expresso pela probabilidade de sucesso de uma determinada ameaça contra uma organização, por exemplo uma estratégia de ataque contra uma rede com milhares de computadores e servidores. A probabilidade de sucesso não é fácil de se medir, no entanto uma termo relacionado "prevalência de vulnerabilidade" é, esse termo representa simplesmente o número de máquinas que são expostas à vulnerabilidade.

- **Custo**

É o impacto que esse risco terá na organização, pode ser classificado como:

- Grandes – São danos "reais" em hardware e software, assim como o tempo da TI para consertar os danos
- Médios – Se refere à danos como perda de negócios ou lentidão nas transações por um certo período.
- Pequenos (leves) – Se referem à perda de performance de sistemas para usuário final, queda na segurança das informações ou impactos menores.

Como aprendemos um número multiplicado por zero terá o resultado igual a zero, portanto qualquer uma dessas variáveis tendo o valor zero o risco será zero.

12 As Mais Recentes Falhas de Segurança Digital

Ninguém quer ser vítima de um ataque cibernético, mas honestamente, ser paranóico o tempo todo também não é divertido. Então, onde está o meio termo feliz? Investir em software antivírus? Em caso afirmativo, qual deles?

Em um mundo cheio de violações de dados e mitos de segurança digital, acreditamos que você deva entender a verdade, então vamos mergulhar em algumas estatísticas sobre o estado de sua segurança cibernética e quebrar as barreiras para ajudá-lo a entender o que realmente está acontecendo .

O que vimos no ano de 2018 pode surpreendê-lo quando se trata de violações de dados e das maiores ameaças à sua segurança digital.

- 92% dos malwares foram entregues por e-mail, não por meio de um navegador.
- Os ataques de phishing foram a principal ameaça de segurança para 56% das pessoas.
- 191 dias foi o tempo médio necessário para identificar violações de segurança.
- Os ataques de ransomware custam às empresas uma média de US $ 5 milhões para serem endereçadas.
- 61% das organizações tiveram que lidar com algum tipo de incidente de segurança do IoT.
- 54 por cento das organizações experimentaram algum incidente de segurança do sistema de controle industrial.

12.1 Dos Ransomwares à Mineração de Dados

Antes do ano de 2018, os atacantes descobriram que, em vez de usar ransomware para exigir pagamentos em Bitcoin ou outras criptomoedas, eles poderiam infectar o computador da vítima com programas de mineração de criptografia. Eles executaram código para roubar moeda

criptografada, comprometendo o desempenho do sistema em todos os lugares.

No início de 2018, o ransomware estava inativo e a criptografia estava em alta. Onde a mineração de criptografia costumava abranger cerca de 10% dos ataques cibernéticos, agora ela era composta por 90% deles. De repente, o software antivírus estava protegendo contra o ransomware, quando precisava evoluir para proteger contra ataques de mineração de criptografia.

12.2 Email e Ataques sem Arquivos

Em 2018, 92% dos malwares ainda eram entregues por e-mail. O malware infecta computadores por meio de ataques de phishing disfarçados de arquivos nos quais você deve clicar para fazer o download. Curiosamente, no entanto, os ataques sem filtro também estavam em ascensão em 2018. O e-mail nem precisava conter um arquivo malicioso para infectar seu computador com malware.

12.3 Segurança Reativa ou Proativa?

Terminamos em 2018 aprendendo com nossas experiências e sendo mais proativos do que reativos, o que é um passo na direção certa. Os fatores mais comuns que levaram a gastos com segurança até o final do ano passado incluem práticas recomendadas, mandatos de conformidade e respostas adequadas aos incidentes de segurança.

Ter um sistema para prevenir ataques usando as melhores práticas, conforme descrito por um conselho de diretores ou uma equipe de gerenciamento, é o primeiro passo, seguido por educar os usuários sobre como responder se houver uma violação de segurança. Com um sistema abrangente em funcionamento, estávamos todos prontos para avançar em 2019.

12.4 Alimentando a Realidade Atual da Segurança Cibernética

É surpreendente que os ataques em dezembro pareçam diminuir quando comparados a todos os outros meses. Os hackers também têm famílias. As

férias são sobre dar, não tomar. Embora sua doação seja provavelmente alimentada por todas as ações que estão fazendo durante os outros períodos.

De qualquer forma, enquanto os fins de semana mostram pouca ou nenhuma atividade de hackers, o resto do mês se mantém estável com um pequeno pico em torno do dia 15. Você pode supor que é o mais seguro em um final de semana no Natal, enquanto é mais vulnerável no meio do mês.

Em ordem do maior para o menor, as técnicas de ataque incluem:

- Malware PoS
- Invasão de conta
- Ataques direcionados
- Vulnerabilidades identificadas
- Injeções de Script
- Recheio de credencial
- Configuração incorreta
- Contas falsas do Facebook
- Malvertising
- Extensões do navegador
- Falsificação de cartão de crédito

Menos de 1% de todas as técnicas de ataque incluem malware, como tradicionalmente pensavamos para nossos computadores pessoais. Isso significa que você precisa ter cuidado com o software antivírus usado para garantir que ele detecte não apenas malwares conhecidos, mas desconhecidos.

12.5 As Maiores Violações de Dados de 2019

Com tudo o que lidamos e aprendemos nos últimos anos, algumas das maiores ocorrências de violações de dados até agora neste ano podem surpreendê-lo. Continue lendo para descobrir quem levou um golpe no departamento de segurança digital em 2019.

12.6 Blur

A Blur, uma empresa de gerenciamento de senhas, relatou uma violação em 2 de janeiro depois que deixou um servidor sem segurança. Apenas

dois dias no ano e já temos que mexer com isso? Sim, e foi rápido. Os hackers obtiveram acesso a 2,4 milhões de endereços de e-mail, nomes de usuários, dicas de senhas, senhas criptografadas e endereços IP.

12.7 Violação de Dados do Jogo Town of Salem

Está acontecendo de novo. Em 3 de janeiro, mais de 7 milhões de jogadores tinham informações roubadas como um servidor contendo endereços de e-mail, nomes de usuário, endereços IP, recursos premium comprados e atividades de jogos comprometidas.

12.8 Quebra de Dados da DiscountMugs.com

Em 4 de janeiro, esse varejista on-line foi invadido por um período de quatro meses inteiros. Eles descobriram um skimming malicioso de cartões no site, onde hackers roubavam números de cartões, códigos de segurança e datas de validade. Eles também obtiveram acesso a informações pessoais, como nomes, números de telefone, endereços e e-mails.

12.9 Violação de Dados do BenefitMall

Em 7 de janeiro, a folha de pagamento, o serviço de empregador e o provedor de RH nos EUA foram vítimas de um ataque de phishing que comprometeu muitas credenciais de login de funcionários, bem como nomes, endereços, datas de nascimento, números de seguro social, contas bancárias e informações de pagamento de prêmios de seguro.

12.10 Violação de Dados da OXO

Ninguém gosta de visitar em uma viagem a Bed, Bath e Beyond mais do que nós. Lençóis macios e os melhores utensílios de cozinha em toda a terra. No entanto, em 10 de janeiro, um dos maiores fornecedores desses produtos sofreu dois incidentes separados com hackers, nos quais as informações dos clientes inseridas em seus sites foram expostas.

12.11 Violação de Dados dos Serviços de Saúde Gerenciados de Indiana

Mais de 31.000 pacientes do sistema de Indiana - Managed Health

Services foram expostos a um ataque de phishing em 11 de janeiro. Hackers ganharam acesso a nomes, endereços, datas de nascimento, números de identificação de seguro e condições médicas.

12.12 Falha de Segurança de Dados do Jogo Fortnite

As falhas no jogo online, Fortnite, expuseram os jogadores a hackers no dia 16 de janeiro. Os hackers poderiam assumir a conta de qualquer um dos 200 milhões de usuários do Fortnite em todo o mundo, obter acesso a informações de contas pessoais, a capacidade de espionar conversas ou comprar notas altas.

12.13 Departamento de Oklahoma - Violação de Dados de Valores Mobiliários

Em 17 de janeiro, milhões de arquivos de agências governamentais, incluindo registros de investigação do FBI, foram encontrados desprotegidos em um servidor aberto no sistema do Departamento de Valores Mobiliários de Oklahoma. Registros que datam de 1986 foram acessados contendo dados pessoais e comunicações internas.

12.14 Coleta de Dados

Um grande banco de dados contendo 773 milhões de e-mails e 22 milhões de senhas foi descoberto no site de armazenamento em nuvem, MEGA, em 17 de janeiro. As informações foram posteriormente compartilhadas em um fórum de hackers onde as pessoas podiam compartilhá-las livremente.

12.15 Violação de Dados da BlackRock Inc.

A BlackRock Inc. é uma das maiores administradoras de ativos do mundo. Em 22 de janeiro, informações sobre 20.000 consultores financeiros vazaram. Documentos de vendas confidenciais foram publicados com nomes, endereços de e-mail e dados financeiros.

12.16 Violação de Dados da Ice Cream - Graeter

A loja online Ice Cream da Graeter continha código malicioso na página de checkout, expondo 12.000 clientes que haviam comprado itens até o dia

22 de janeiro. Entre as informações obtidas estavam nomes, números de telefone, endereço, números de fax e informações de pagamento.

12.17 Locais de Apostas Online - Violação de Dados

Os sites de apostas informativas azur-casino.com, kahunacasino.com, viproomcasino.net e easybet.com copiaram 108 milhões de registros de clientes para um serviço de armazenamento em nuvem em 23 de janeiro, sem protegê-los. As informações expostas incluíam nomes, números de telefone, endereços, e-mails, nomes de usuário, datas de nascimento, saldos de contas, detalhes do navegador e do S.O., endereços IP e informações sobre ganhos e perdas.

12.18 Violação de Dados da Ascension

Nas duas semanas anteriores a 23 de janeiro, 24 milhões de documentos bancários e hipotecários ficaram desprotegidos em um banco de dados on-line. A empresa de análise de dados Ascension foi responsável pelo vazamento que incluía nomes, datas de nascimento, endereços, números do seguro social e outras informações financeiras.

12.19 Departamento de Saúde e Serviços Sociais do Alasca com Violação de Dados

Os hackers tiveram como alvo o Departamento de Saúde e Serviços Sociais do Alasca, expondo dados sobre 100.000 pessoas em 23 de janeiro. Eles ganharam acesso a nomes, datas de nascimento, endereços, números do seguro social, informações de saúde e informações sobre renda.

12.20 Falha de Segurança da Rubrik

Rubrik é um provedor de segurança de TI e gerenciamento de dados em nuvem. Em 29 de janeiro, eles tiveram um enorme vazamento de banco de dados envolvendo informações de clientes. O vazamento ocorreu em um servidor do Amazon Elasticsearch que não exigia senha.

12.21 Violação de Dados de Saúde no Colorado

Uma unidade de saúde com sede no Colorado expôs informações pessoais

de saúde depois que os funcionários foram vítimas de um ataque de phishing. Cerca de 23.000 pessoas foram expostas, incluindo nomes, datas de nascimento, endereços, números da Previdência Social, informações médicas e carteiras de habilitação.

12.22 Proteção Digital para o Futuro

E isso foi apenas violações de dados para o mês de janeiro de 2019. A lista continua incluindo Houzz, Catawba Valley Medical Center, Huddle House, Parceiros EyeSouth, Dunkin 'Donuts, Coffee Meets Bagel, 500px, North Country Business Products, Advent Health, Coinmama, UW Medicine, UConn Health, Dow Jones, Rush University Medical Center e Health Alliance Plan nos meses de fevereiro e março.

Então, com toda essa informação em mãos, como será o futuro? Como evidenciado por nossas estatísticas de 2018, já sabemos que 2019 e posteriores não mostrarão uma diminuição de ataques cibernéticos mais sofisticados por meio de novos métodos.

Aqui estão algumas das áreas onde você pode esperar problemas de segurança no futuro...

12.23 Biometria

O número um no radar deve ser o roubo de dados biométricos. Quanto mais usamos nossas impressões digitais, scanners de íris ou reconhecimento facial para aumentar a segurança, mais nos arriscamos a esses recursos serem roubados. O que antes era uma solução para problemas de segurança cibernética, agora se tornou um alvo para hackers em todos os lugares.

Como os hackers podem manipular sensores, os dados biométricos podem ser alterados, permitindo que eles aproveitem as falhas presentes nos dispositivos de autenticação biométrica e no hardware. No futuro, as entidades de saúde, financeiras e governamentais são as que estão em maior risco. As organizações precisam fazer tudo o que puderem para garantir que os dados biométricos sejam criptografados em todos os níveis, em todas as camadas.

No momento, não há muita regulamentação sobre o armazenamento de dados biométricos, mas isso precisa mudar imediatamente. Scanners, sensores e outros hardwares biométricos devem estar melhor equipados para detectar e lidar com anomalias como parte de qualquer sistema de autenticação multifator.

12.24 Skimming

Skimming não é uma nova tecnologia. Os hackers vêm desbancando caixas eletrônicos para obter números de cartões em todo o mundo já faz algum tempo. Mas agora eles obtem de forma digital. O Skimming Malware permite que os criminosos baixem informações de cartão de crédito diretamente de sites de comércio eletrônico em qualquer lugar. Compras on-line aumentaram em popularidade, tornando-se um alvo lucrativo.

O malware usado para explorar esses números de sites de comércio eletrônico tem sido praticamente indetectável até o momento. Avançando, esses sites precisam monitorar de perto suas redes em busca de comportamentos incomuns e anomalias, especialmente se estiverem envolvidas informações de clientes.

12.25 Celulares

Os telefones celulares são essenciais para nossa vida cotidiana e, como todos precisam rastrear um celular, é esse número de telefone, as operadoras de telefonia celular devem procurar violações de dados e melhorar a segurança.

Com um conjunto de informações muito simples, os hackers podem acessar chamadas telefônicas e mensagens de texto, descobrindo informações pessoais e distribuindo-as por toda a Internet. A penetração das camadas de segurança da rede SS7 também permite que os hackers acessem informações de localização. Cabe aos fabricantes e operadoras de telefonia celular melhorar a segurança da SS7 trabalhando juntos para o benefício de todos.

12.26 Jogos Online

Em 2011, vimos uma violação do Playstation da Sony, o que nos deu um vislumbre das vulnerabilidades no mundo dos jogos. Muitos jogadores apenas empregam o uso de uma senha e passam por um simples identificador on-line, tornando-os alvos fáceis para hackers. Ao obter acesso à conta de um jogador, eles podem se passar por um avatar familiar e obter informações privilegiadas.

Não apenas os cartões de crédito dos jogadores estão em risco, mas armas, tokens e outros itens de jogos são incrivelmente valiosos no mundo dos jogos. A segurança cibernética no mundo dos jogos começa com a educação do usuário. Muitos jogadores mais jovens não entendem a importância de se manter seguros on-line, e os fabricantes de jogos precisam de autenticações, hardware e redes mais fortes.

12.27 O que Você Pode Fazer para Ficar em Segurança Online?

O principal objetivo aqui é que você precisa mais do que apenas um olhar atento. Você precisa ser proativo para proteger a si mesmo ou sua empresa contra as ameaças mais recentes de segurança cibernética. Um provedor abrangente de antivírus, VPN e proteção contra roubo de identidade pode fornecer as ferramentas necessárias para monitorar e se preparar para um ataque. Também pode ajudá-lo a recuperar se o pior acontecer.

Não só você deve tomar as precauções necessárias para se proteger, mas você precisa envolver uma empresa respeitável, com um bom histórico de prestação de um serviço. Nem todas as empresas oferecem os mesmos serviços, nem fornecem os mesmos planos abrangentes de proteção.

Sua capacidade de pensar criticamente e responder adequadamente garantirá que suas informações pessoais e ativos financeiros permaneçam seguros. Ele irá protegê-lo contra roubo de identidade, ataques contínuos ou algo pior. Coloque em prática o que você aprendeu neste artigo para se manter protegido contra as ameaças de segurança cibernética mais prováveis de 2019.

13 Gestão de Riscos e Segurança da Informação

O volume de informações eletrônicas utilizadas pelas empresas é cada vez maior, tornando complexo seu gerenciamento produtivo e adequação da qualidade de acesso, confiabilidade e conformidade com vistas a atender os objetivos organizacionais, assim como há a preocupação com sua exposição, cuja segurança pode ser comprometida por incidentes que representariam prejuízos financeiros ou para a imagem das organizações (POSTHUMUS & VON SOLMS, 2004)

Para Sêmola (2003), a gestão da segurança da informação pode ser classificada em três aspectos: tecnológicos, físicos e humanos. As organizações preocupam-se principalmente com os aspectos tecnológicos (redes, computadores, vírus, *hackers*, Internet) e se esquecem dos outros - físicos e humanos - tão importantes e relevantes para a segurança do negócio quanto os aspectos tecnológicos.

As organizações processam informações sobre funcionários, clientes, fornecedores, pacientes ou alunos. As informações podem estar relacionadas apenas a seus nomes e endereços, mas geralmente incluem números de seguridade social, números de cartão de crédito, detalhes de contas bancárias, informações de saúde, etc. Se a informação é acessada ou divulgada a partes não autorizadas, isso pode acarretar em multas, processos civis ou até mesmo penas de prisão; além disso, a reputação da organização pode ser prejudicada, podendo levar a perdas financeiras (DA VEIGA & MARTINS, 2015).

O gerenciamento de riscos tem como objetivos a identificação das ameaças e a quantificação dos riscos inerentes à segurança da informação, além do desenvolvimento de um plano de ação. Os autores Liu et al. (2018) identificaram que a avaliação da qualidade da informação, informações do ambiente e monitoramento de segurança influenciam na identificação do risco, juntamente com a associação e integração de informações atuando como mediadores resultando no gerenciamento do risco. Assim, as organizações devem garantir o controle dos dados e informações através do gerenciamento de riscos (CALVARD & JESKE, 2018).

A Figura 1 apresenta o conjunto de atributos que influenciam na segurança

e privacidade da informação, considerando influências internas e externas:

Figura 1 – Atributos da informação pela perspectiva da privacidade e segurança da informação

Fonte: DA VEIGA (2015, apud SOUZA, 2016)

A segurança da informação e a privacidade da informação estão estreitamente alinhadas.

13.1 Etapas da Análise de Risco

O termo 'Análise de Risco', inserido no contexto da segurança da informação, pode ser entendido como o "processo que identifica e avalia de forma sistemática, metodológica e repetível os riscos de segurança a que os recursos críticos de negócio das organizações se encontram sujeitos, possibilitando a definição dos meios através dos quais estes podem ser protegidos".

A realização de uma análise de risco compreende as seguintes etapas:

- Identificação dos recursos considerados críticos para a atividade e sobrevivência da organização, recursos estes que são valorizados de acordo com a sua relevância para o negócio;
- Identificação das vulnerabilidades que se encontram associadas a

estes recursos e das ameaças a que estes se encontram expostos, bem como a sua probabilidade de ocorrência e impacto esperado;
- Determinação, o mais realista possível, das perdas e danos (tangíveis e intangíveis) associados aos impactos resultantes da concretização de uma ou mais ameaças, sobre um dado recurso. Deste cálculo decorre o nível de risco associado ao recurso em questão.
- De acordo com o nível de risco identificado, segue-se a classificação deste quanto à sua aceitação ou necessidade de mitigação, atendendo ao grau de conforto pretendido pela organização.
- Um nível de risco pode ser aceito caso a organização decida que este não acarreta consequências significativas para a concretização das suas atividades de negócio, sendo que a aceitação de um determinado nível de risco pode, contudo, presumir a realização de esforços no sentido de mitigá-lo, reduzindo-o a um valor considerado aceitável para a organização.

No sentido de reduzir a probabilidade de verificação de um determinado nível de risco sobre um recurso, as suas consequências, ou mesmo facilitar o restauro do normal funcionamento desse mesmo recurso e atividades associadas, as organizações devem definir e implementar medidas de segurança da informação.

O grau de risco que permanece após o processo de 'Tratamento do Risco', quer envolva a mitigação, eliminação, transferência ou simples aceitação da presença desse mesmo risco, é usualmente denominado de 'nível de risco residual' ou 'nível de risco aceitável'.

É importante referir que uma análise de risco está intimamente relacionada com a análise custo/benefício da implementação (ou não) dos controles considerados necessários ou adequados aos requisitos de segurança da informação da organização.

Outro aspecto importante é a necessidade da realização regular de análises de risco. É indispensável o monitoramento do nível de risco, de forma a garantir a eficiência e a eficácia da gestão desse mesmo risco, processo que compreende, tanto a análise, como o tratamento dos riscos identificados previamente.

14 Alguns Conceitos de Gestão da Informação

14.1 Relatos do Surgimento do Gerenciamento de Informações

Segundo Davenport (1998), são os governos os pioneiros na efetuação desse gerenciamento. Os primeiros repositórios sumérios datam de 5.000 a.c. A França cria um escritório nacional de registros, no século XVIII, a Inglaterra no XIX e os Estados Unidos, no século XX. As organizações começam a administrar as informações em meados da década de 40, mantendo até hoje unidades de gerenciamento. Entretanto, o que é recente é a forma consciente de gerir o conhecimento.

14.2 Surgimento do Conceito

O termo “gestão da informação” surge nos anos oitenta, nos Estados Unidos e na Inglaterra, como Gerência dos Recursos Informacionais, com foco em gerenciar a informação como recurso estratégico, tendo como marco a publicação do documento US Public Act A130 pelo Governo dos Estados Unidos4 (CIANCONI, 1999).

14.3 Alguns Conceitos de Gestão da Informação

1) A Gestão da Informação que, para Dias e Belluzzo (2003, pg.65), “É o conjunto de conceitos, princípios, métodos e técnicas utilizados na prática administrativa e colocados em execução pela liderança de um serviço de informação [...] para atingir a missão e os objetivos fixados previamente”.

2) Gestão da Informação “é um conjunto de processos que englobam atividades de planejamento, organização, direção, distribuição e controle de recursos, visando à racionalização e à efetividade de determinado sistema, produto ou 17 serviço”.

3) Segundo Reis (1993), "Para que esta gestão [de informação] seja eficaz, é necessário que se estabeleçam um conjunto de políticas coerentes que possibilitem o fornecimento de informação relevante, com qualidade

suficiente, precisa, transmitida para o local certo, no tempo correcto, com um custo apropriado e facilidades de acesso por parte dos utilizadores autorizados".

4) Berbe (2005) define a atividade de Gestão da Informação da seguinte maneira: A atividade de gestão pode ser considerada como um conjunto de processos que englobam atividades de planejamento, organização, direção, distribuição e controle de recursos. Nas empresas esses recursos podem ser econômicos, materiais, tecnológicos informacionais, humanos e de qualquer outra espécie. Toda gestão visa racionalizar e melhorar a eficiência das atividades que envolvem uma organização (BERBE, 2005, p. 26).

5) Segundo Davenport (1997), pode-se conseguir melhorias do processo de Gestão da Informação com a adoção de uma abordagem “ecológica”. Ou seja, deve-se encarar o processo do ponto de vista do ambiente como um todo: arquitetura e tecnologia da informação; estratégias, políticas e comportamentos ligados à informação; processos de trabalho; e pessoas. Uma abordagem ecológica envolve:

- integração de diversos tipos de informação (estruturada, não estruturada, automatizada, não-automatizada, textos, áudio, vídeo, etc.) e reconhecimento das tendências à mudança;
- ênfase na observação e descrição;
- foco nas pessoas e no comportamento informacional.

15 Contexto da Gestão da Informação no Espaço Profissional

Segundo Marchiori (2002) as tecnologias da informação e da comunicação têm possibilitado a convergência dos tradicionais suportes informativos, assim como a criação de outros objetos ou representações de informação, que já iniciam em um ambiente virtual. Assim sendo, tais tecnologias provocam e exigem uma mudança quanto as profissões e áreas que antes eram razoavelmente estanques. Em um mundo que tendencia a ser altamente interconectado, e que para tal necessita de padrões e procedimentos, do desenvolvimento estruturado de conteúdos informativos, de alta capacidade de gerenciamento e de habilidades de mediação, as demandas são tão dinâmicas como heterogêneas.

Aos profissionais da informação ditos “tradicionais” (como os arquivistas, os bibliotecários, os museólogos, os profissionais dos meios de comunicação de massa e até mesmo os informáticos) se agregam outros, ditos “emergentes”, o que indica a forte necessidade de interação de habilidades e conhecimentos técnicos e gerenciais disponíveis na arena de profissionais de informação e de outras áreas, tais como educação, marketing, história, administração, economia, entre outros. Os exemplos se multiplicam, e independentemente de formações técnicas ou de nível superior (e mesmo de complementação/extensão e de pós-graduação), tais indivíduos se posicionam no campo de atividades de informação sob variados títulos, tais como web designers, engenheiros de conteúdo, arquitetos de informação (apenas para exemplificar) – advogando, não raras vezes com propriedade, que dominam técnicas, modelos e metodologias que, se não são de todo inéditas (sob o ponto de vista de que o ciclo de vida e de gerência da informação é comum àqueles que partilham do mesmo campo de atividades), apresentam respostas efetivas aos problemas crescentes relativos à gerência dos dados, da informação e, mais recentemente, do que vem se chamando de “gestão do conhecimento” segundo Dillon (2001).

Nem todas estas ocupações/funções demandadas, no momento, serão mantidas em um futuro próximo, pois a história e a experiência confirmam que profissões e/ou ocupações dependentes intensivamente de uma tecnologia têm dificuldades de se manterem e de se modificarem quanto tal tecnologia é substituída e/ou se esgota. Todavia, o campo de atividades de informação tem crescido o suficiente para abrigar novos profissionais, desafiando suas habilidades em contextos cada vez mais dinâmicos Horton Jr (1992).

16 Referências

Associação Brasileira de Normas Técnicas (ABNT). NBR ISO/IEC 27002:2005 – Tecnologia da informação – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BERBE, Alexandre Campos. Gestão da Informação e do conhecimento. Reflexão de conceitos e o papel da Biblioteconomia. 2005. 103 f. Monografia (Bacharelado em Biblioteconomia) – Universidade de São Paulo, São Paulo, 2005.

BROWN, Leslie R. et al. Knowledge Integrator Nodes in Teams or Networks in Multinational. In IMP GROUP ASIA CONFERENCE PROCEEDINGS, 2002, Perth, Austrália, Disponível em: https://eprints.usq.edu.au/981/1/Erwee_Brown_Poh.pdf. Acesso em 30 jun. 2016.

CALVARD, Thomas Stephen; JESKE, Debora. Developing human resource data risk management in the age of big data. International Journal of Information Management, v. 43, p. 159-164, 2018.

CAPURRO, Rafael; HJORLAND, Birger. O conceito de informação. Perspect. ciênc. inf., Belo Horizonte, v. 12, n. 1, Apr. 2007.

CHAFFEY, Dave; WOOD, Steve. Business information management. Improving performance using information systems. Essex : Harlow, 2005.

CIANCONI, R. Gestão da informação na sociedade do conhecimento. Brasília, DF: SENAI/DN, 1999.

DA SILVA NETTO, Abner; DA SILVEIRA, Marco Antonio Pinheiro. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. JISTEM-Journal of Information Systems and Technology Management (Online), v. 4, n. 3, p. 375-397, 2007.

DA VEIGA, Adéle; MARTINS, Nico. Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review, v. 31, n. 2, p. 243-256, 2015.

DANTAS, Marcus Leal, Segurança da Informação: uma abordagem focada em gestão de riscos.Livro Rápido/Olinda,2001.

DAVENPORT, T.; PRUSAK, L. Conhecimento empresarial: como asorganizações gerenciam o capital intelectual. Rio de Janeiro: Campus, 1998.

DAVENPORT, Thomas H. Information Ecology. Oxford: Oxford University Press, 1997.

DAVENPORT, Thomas H. Thinking for a living: how to get better

performances and results from knowledge workers. Harvard Business School Press. Boston. Massachussets. 2005.

DAVENPORT, Thomas H.; PRUSAK, L. Working knowledge: How organizations manage what they know. Harvard Business School Press, Boston 2000.

DIAS, M. M. K; BELLUZZO, R. C. B. Gestão da informação em ciência e tecnologia sob a ótica do cliente. Bauru: EDUSC, 2003.

DILLON, Andrew. (2001) I think therefore IA? American Society for Information Science and Technology, v. 27, n. 2, Dec./Jan.

DONOGHUE, Leigh P.; HARRIS, Jeanne G.; WEITZMAN, Bruce A. Knowledge management strategies that create value. Outlook, v. 1, n. 1, p. 48-53, 1999.

DRUCKER, Peter. Além da revolução da informação. HSM Management, v. 18, p. 48-55, jan./fev. 2000.

GEISLER, E. A typology of knowledge management: strategic groups and role behavior in organizations. Journal of Knowledge Management, v. 11, n. 1, p. 84–96, 2007.

GIL, A. L. Sistema de Informações Contábil/Financeiros. 3ª Ed. São Paulo: Atlas, 1999.

HÄDRICH, Thomas. Situation-oriented Provision of Knowledge Services. Information Systems, 2008. Disponível em https://sundoc.bibliothek.uni-halle.de/diss-online/08/08H128/prom.pdf Acessado em 30 mar. 2019.

HARJINDER, G; RAO, P.C The oficial design the data warehousing, :Que Corporation, 1996.

HASSAN, E.; Yusof, Z. M.; Ahmad, K. Determinant Factors of Information Quality in the Malaysian Public Sector. In: Proceedings of the 2018 9th International Conference on E- business, Management and Economics. ACM, 2018. p. 70-74.

HORTON JUNIOR, Forest Woody. (1992) Needs and careers in

information services. FID News Bulletin, v. 42, n. 2, p. 32-34, Feb.

https://www.information-management.com/opinion/the-biggest-data-breaches-and-digital-security-threats-of-2019?regconf=1. Acessado em 24/04/2019.

https://www.information-management.com/opinion/the-growing-legal-and-regulatory-implications-of-collecting-biometric-data. Último acesso em (06/05/2019).

ISO/IEC 13335-1:2004 – Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.

LAUDON, K. C.; LAUDON, J. P. Sistemas de informação gerenciais: administrando a empresa digital. São Paulo: Pearson Prentice Hall, 2004.

LIU, Lu; LIU, Xinlei; LIU, Guangchen. The risk management of perishable supply chain based on coloured Petri Net modeling. Information processing in agriculture, v. 5, n. 1, p. 47-59, 2018.

MACEDO, Valéria; SANTOS, Neusa M. B. F. dos; JOÃO, Belmiro do N.; SAITO, André; Tipologia do Trabalhador do Conhecimento: Papéis e Processos. 2016. Disponível em http://www.periodicos.ufpb.br/ojs/index.php/pgc/article/download/33081/1 Acessado em 30 de mar. 2019.

MARCHIORI, P. (2002) - A ciência da informação: compatibilidade no espaço profissional. Caderno de pesquisas em Administração, São Paulo, v.9, n.1, p.91-101, jan./mar.

MOORE, Connie; RUGULLIES, Erica. The information workplace will redefine the world of work at last. Forrester Big Idea, 2005.
Oliveira, D. P. R. (2005). Sistemas de Informações Gerenciais. São Paulo, Editora Atlas S. A.

PIMENTA, R. C. de Q. Gestão da informação: um estudo de caso em um instituto de pesquisa tecnológica. Dissertação (Mestrado em Administração) - Universidade Federal do Rio Grande do Norte, Natal,

2008.

POSTHUMUS, Shaun; VON SOLMS, Rossouw. A framework for the governance of information security. Computers & security, v. 23, n. 8, p. 638-646, 2004.

Reis, Carlos (1993)- Planeamento Estratégico de Sistemas de informação. Lisboa 1993 ia ed. ed. Presença. pg.20-24.

REZENDE, Denis Alcides; ABREU, Aline França de. Tecnologia da Informação aplicada a sistemas de Informação Empresariais. 6 ed. São Paulo: Atlas, 2014.

ROSSINI, Alessandro Marco. PALMISANO, Angelo. Administração de sistemas de Informação e a Gestão do Conhecimento; São Paulo, Pioneira Thomson; 2012.

SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma Visão Executiva. Rio de Janeiro: Ed. 2003.

SOUZA, Jackson Gomes Soares et al. Gestão de Riscos de Segurança da Informação numa Instituição Pública Federal: um estudo de caso. Revista Eniac Pesquisa, v. 5, n. 2, p. 240-256, 2016.

STAIR, R. M.; REYNOLDS G. W. Princípios de Sistemas de Informações: Uma abordagem Gerencial. 4º ed. São Paulo: LTC, 2002.

TURBAN, Efraim; Rainer Jr., R. Kelly & Potter, Richard E.; tradução Daniel Vieira. Introdução a Sistemas de informação. Rio de Janeiro: Elseier, 2007.

VALENTIM, Marta L.P. Gestão da informação e gestão do conhecimento. Marília, 2004. Artigo, Info Home. Disponível em: < http://www.ofaj.com.br/colunas_conteudo.php? cod=88 >.