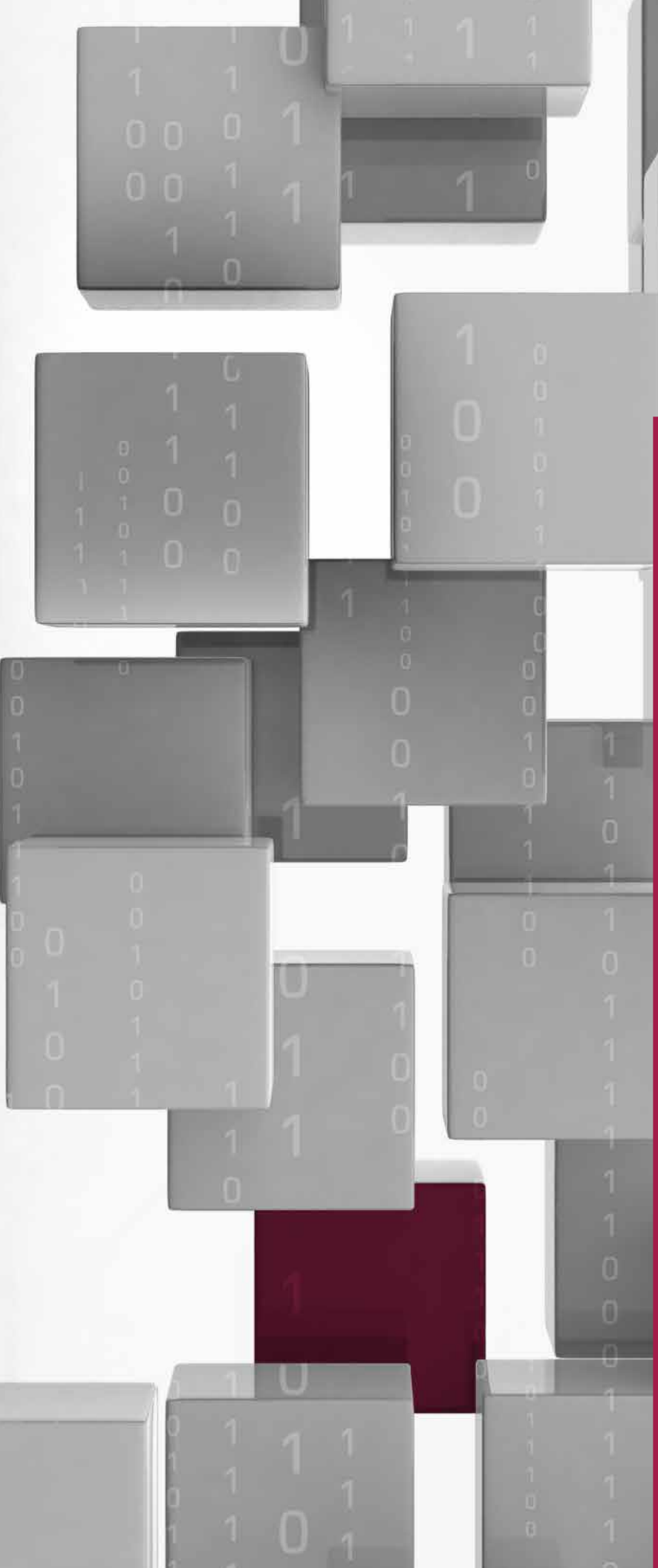


ISACA®
Trust in, and value from, information systems

PRIVACIDADE & BIG DATA

ARTIGO DA ISACA DE AGOSTO DE 2013

Melhoria na tomada de decisão, tempo mais rápido para comercialização, melhor serviço ao cliente e aumento nos lucros são apenas alguns dos benefícios que contribuíram para a explosão da implementação de big data em empresas de todos os tamanhos. O Fórum Mundial Econômico descreve as informações pessoais armazenadas pelo big data como “o novo ‘petróleo’ - um recurso valioso do século XXI”. A analítica do big data é o “novo motor da criação de valor socioeconômico”. As empresas desejam colher os benefícios de big data e seu vasto potencial é reconhecer sua responsabilidade para proteger a privacidade dos dados pessoais coletados e analisados pelo Big Data. Mecanismos adequados de manutenção e risco para governar e proteger a privacidade necessária serão áreas principais de foco em toda iniciativa de Big Data. A ampla estrutura comercial de COBIT®5 para a governança de TI empresarial mantém um equilíbrio entre realizar benefícios e otimizar os níveis de risco e uso de recurso.

ISACA®

Com mais de 110.000 clientes em 180 países, a ISACA *(www.isaca.org)* ajuda os líderes comerciais e de TI a maximizarem o valor e gerenciar o risco relacionado à informação e tecnologia. Fundada em 1969, a ISACA, independente e sem fins lucrativos, é uma defensora para profissionais envolvidos em segurança da informação, garantia, gerenciamento de risco e governança. Esses profissionais confiam na ISACA como fonte confiável de informações e conhecimento tecnológico, comunidade, normas e certificação. A associação, que tem 200 capítulos em todo o mundo, aprimora e atesta habilidades e conhecimentos em TI por meio de suas designações globalmente reconhecidas Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) eCertified in Risk and Information Systems Control™ (CRISC™). A ISACA também desenvolveu e atualiza continuamente o COBIT®, uma estrutura de negócios que ajuda as empresas em todas as indústrias e geografias a governarem e gerenciarem suas informações e tecnologia.

Isenção de responsabilidade

A ISACA designou e criou a *Privacidade e Big Data* (o "Artigo"), principalmente como recurso educacional para profissionais de governança e qualidade. A ISACA não garante que o uso de qualquer parte do Artigo assegure o sucesso do resultado. Não se deve considerar que o Artigo inclua todas as informações, procedimentos e testes apropriados ou exclua outras informações, procedimentos e testes voltados razoavelmente para a obtenção dos mesmos resultados. Ao determinar a adequação de qualquer informação, procedimento ou teste específico, os profissionais de governança e qualidade devem aplicar seu próprio juízo profissional às circunstâncias específicas apresentadas pelos sistemas ou ambientes de tecnologia da informação em questão.

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EUA

Fone: +1 847 253-1545

Fax: +1 847 253-1443

E-mail: *info@isaca.org*

Site: *www.isaca.org*

Dê sua opinião:
www.isaca.org/privacy-and-big-data

Participe do Centro de conhecimento da ISACA:
www.isaca.org/knowledge-center

Siga a ISACA no Twitter:
https://twitter.com/ISACANews

Conecte-se à ISACA no LinkedIn:
ISACA (Oficial)
http://linkd.in/ISACAOfficial

Curta a ISACA no Facebook:
www.facebook.com/ISACAHQ

AGRADECIMENTOS

A ISACA gostaria de agradecer aos seguintes colaboradores:

Equipe de desenvolvimento de projeto

Mario Bojilov
CISA, Meta Business Systems, Austrália

Richard Chew
CISA, CISM, CGEIT, Emerald Management Group, EUA

Francis Kaitano
CISA, CISM, CEN, Nova Zelândia

Tichaona Zororo
CISA, CISM, CGEIT, CRISC, EGIT, África do Sul

Revisores especialistas

Todd Atteberry
The Atteberry Group, EUA

Goutama Bachtiar
Global Innovations and Technology Platform, Indonésia

Graciela Braga
CGEIT, Argentina

Girish Netke
CISA, A-N-G Computer Consultants, Índia

Diretoria da ISACA

Tony Hayes
Vice-presidente CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Governo de Queensland, Austrália, Presidente Internacional

Allan Boardman
Vice-presidente CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, Reino Unido

Juan Luis Carselle
Vice-presidente CISA, CGEIT, CRISC, Wal-Mart, México

Ramses Gallego
Vice-presidente CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Espanha

Theresa Grafenstine
CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, EUA, Vice-Presidente

Vittal Raj
CISA, CISM, CGEIT, CFE. CIA, CISSP, FCA, Kumar & Raj, Índia, Vice-Presidente

Jeff Spivey
Vice-presidente CRISC, CPP, PSP, Security Risk Management Inc., EUA

Marc Vael, Ph.D.
CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Bélgica, Vice-Presidente

Gregory T. Grocholski
CISA, The Dow Chemical Co., EUA, Ex-Presidente Internacional

Kenneth L. Vander Wal
Ex-Presidente internacional CISA, CPA, Ernst & Young LLP (aposentado), EUA

Christos K. Dimitriadis, Ph.D.
CISA, CISM, CRISC, INTRALOT S.A., Grécia, Director

Krysten McCabe
Diretor CISA, The Home Depot, EUA

Jo Stewart-Rattray
Diretor CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Austrália

Diretoria técnica

Christos K. Dimitriadis, Ph.D.
CISA, CISM, CRISC, INTRALOT S.A., Grécia, Diretor

Rosemary M. Amato
CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., Holanda

Steven A. Babb
CGEIT, CRISC, Betfair, Reino Unido

Thomas E. Borton
CISA, CISM, CRISC, CISSP, Cost Plus, EUA

Phil J. Lageschulte
CGEIT, CPA, KPMG LLP, EUA

Anthony P. Noble
CISA, Viacom, EUA

Jamie Pasfield
CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, Reino Unido

Comitê de orientação e práticas

Phil J. Lageschulte
Presidente CGEIT, CPA, KPMG LLP, EUA

John Jasinski
CISA, CGEIT, ISO20K, ITIL Exp, SSBB, ITSMBP, EUA

Yves Marcel Le Roux
CISM, CISSP, CA Technologies, França

Aureo Monteiro Tavares Da Silva
CISM, CGEIT, Brasil

Jotham Nyamari
CISA, CISSP, Deloitte, EUA

James Seaman
CISM, RandomStorm, Reino Unido

Gurvinder Singh
CISA, CISM, CRISC, Austrália

Siang Jun Julia Yeo
CISA, CPA (Austrália), MasterCard Asia/Pacific Pte. Ltd., Cingapura

Nikolaos Zacharopoulos
CISA, CISSP, DeutschePost–DHL, Alemanha

ISACA e afiliados e patrocinadores do ITGI® (IT Governance Institute®)

Information Security Forum
Institute of Management Accountants Inc.
Filiais da ISACA
ITGI França
ITGI Japão
Universidade de Norwich
Socitum Performance Management Group
Faculdade de Economia e Administração Solvay, Bruxelas
STMI (Strategic Technology Management Institute) da Universidade Nacional de Cingapura
Faculdade de Administração da Universidade de Antuérpia

ASIS International
Hewlett-Packard
IBM
Symantec Corp.

Introdução

O Big Data pode ser bem poderoso e ter um impacto positivo e negativo significativo em uma empresa. **Melhoria na tomada de decisão, tempo mais rápido para comercialização, melhor serviço ao cliente e aumento nos lucros são apenas alguns dos benefícios que contribuíram para a explosão da implementação de big data em empresas de todos os tamanhos.** As violações de privacidade de Big Data podem resultar em consequências jurídicas dispendiosas para as empresas.

A definição de Big Data foi dada pela primeira vez em um artigo de Doug Laney.[1] Ele definiu Big Data como conjuntos de dados com três aspectos que introduzem desafios de processamento específico: volume, velocidade e variedade. A velocidade é a rapidez com que os dados são criados. Esta velocidade está aumentando drasticamente. Durante cada minuto em 2012, os consumidores gastaram US$ 272.000,00 em compras pela Internet e as marcas receberam 34.722 "curtidas" no Facebook. A variedade se refere aos diferentes tipos de dados que estão sendo processados. Esses mudaram de arquivos simples e banco de dados relacional para áudio, vídeo, informação de sensor etc. O volume é o resultado do aumento de variedade e velocidade. Hoje, as empresas estão processando terabytes e petabytes de informação.

Em 2013, a ISACA definiu Big Data como conjuntos de dados que são muito grandes ou com rápidas mudanças para serem analisados com técnicas de banco de dados relacionais tradicionais ou multidimensionais ou ferramentas de software comumente usadas para capturar, gerenciar e processar os dados em um tempo razoável. "O Big Data representa uma tendência em tecnologia que está abrindo caminho para um novo método de compreensão do mundo e do processo decisório de negócios."[2]

O Fórum Econômico Mundial descreve as informações pessoais coletadas pelo Big Data como "o novo 'petróleo' - um recurso valioso do século XXI", e a análise desses dados como "o novo motor da criação de valor socioeconômico."[3,4]

As empresas desejam colher os benefícios de big data e seu vasto potencial é reconhecer sua responsabilidade para proteger a privacidade dos dados pessoais coletados e analisados pelo Big Data. Mecanismos adequados de manutenção e gestão de risco para governar e proteger a privacidade necessária serão áreas principais de foco em toda iniciativa de Big Data. A ampla estrutura comercial de COBIT 5 para a governança de TI corporativa mantém um equilíbrio entre realizar benefícios, otimizar os níveis de risco e uso de recurso. Esta estrutura pode ser aplicada com bastante sucesso às exigências de privacidade de Big Data e aos seus desafios.

Este artigo foca o impacto do Big Data em privacidade, risco de privacidade, estratégias de privacidade de Big Data, considerações de governança e segurança para privacidade de Big Data.

---

[1] Laney, Doug; "3D Data Management: Controlling Data Volume, Velocity and Variety", gartner.com, 6 de fevereiro de 2001, *www.blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf*

[2] ISACA.org, "Big Data: Impacts and Benefits", Março de 2013, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Big-Data-Impacts-and-Benefits.aspx*

[3] World Economic Forum, "Personal Data: The Emergence of a New Asset Class", Janeiro de 2011, *www.weforum.org/reports/personal-data-emergence-new-asset-class*

[4] World Economic Forum, "Unlocking the Value of Personal Data: From Collection to Usage", Fevereiro de 2013, *www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf*

Impactos de Big Data na Privacidade

Em todas as indústrias, incluindo bancos, governo, saúde, mídia, energia e educação, a automação exponencial dos processos comerciais está expandindo a paisagem do consumo e análise de dados.

Na busca das empresas em oferecer o retorno sobre investimento (ROI) de Big Data aceitável e mensurável, os dados que foram armazenados em depósitos on-line e off-line diferentes, em vários formatos, agora estão disponíveis em formato digital, prontos para serem correlacionados, agregados e analisados estatisticamente em grandes blocos de terabytes e petabytes em tempo real.

Como o volume de dados, a velocidade de processamento, a complexidade do tipo de dados e as especificações de segurança e privacidade continuam a crescer além das expectativas, as empresas são forçadas a buscar novas maneiras de atender as necessidades operacionais, comerciais e jurídicas.

O Big Data é uma força significativa por trás do crescente número de empresas que estão tomando a decisão de passar os dados para a nuvem e usar serviços analíticos baseados em Cloud, além do processamento analítico de bancos de dados, tais como Processamento Paralelo em Grande Escala (MPP) ou Multiprocessamento Simétrico (SMP).

O Big Data iniciou as discussões sobre a privacidade internacional e as leis de proteção aos dados. Atualmente, cada região (União Europeia, EUA etc.), o governo e a empresa manuseiam a privacidade e a proteção de dados de maneiras diferentes. Este impacto geopolítico forçou as empresas a reconsiderar a maneira como lidam e protegem a privacidade dos indivíduos e as informações coletadas sobre eles e como as empresas implementam suas soluções de Big Data com base na nuvem.

A adoção de Big Data também está influenciando a maneira como as empresas entregam seus projetos de TI. A maioria dos projetos de Big Data tem muita tecnologia e dados. A tecnologia é complicada e as habilidades necessárias para oferecê-la são relativamente escassas, o que resultou em estouros nos orçamentos do projeto.

O crescimento de Big Data levou a diferentes repositórios de armazenamento os registros pessoais de saúde e os detalhes de transações de cartão de crédito. O armazenamento e a análise desses dados aumentaram a pressão sobre as organizações, para que estejam de acordo com as regulamentações de privacidade, como a Norma de Segurança de Dados da Indústria de Cartão de Pagamento (PCI DSS), a Lei de Proteção de Dados do Reino Unido, de 1998, e a Lei de Responsabilidade e Portabilidade de Seguro de Saúde dos EUA (HIPAA). É necessária uma abordagem pragmática para considerar essas especificações de conformidade de Big Data.

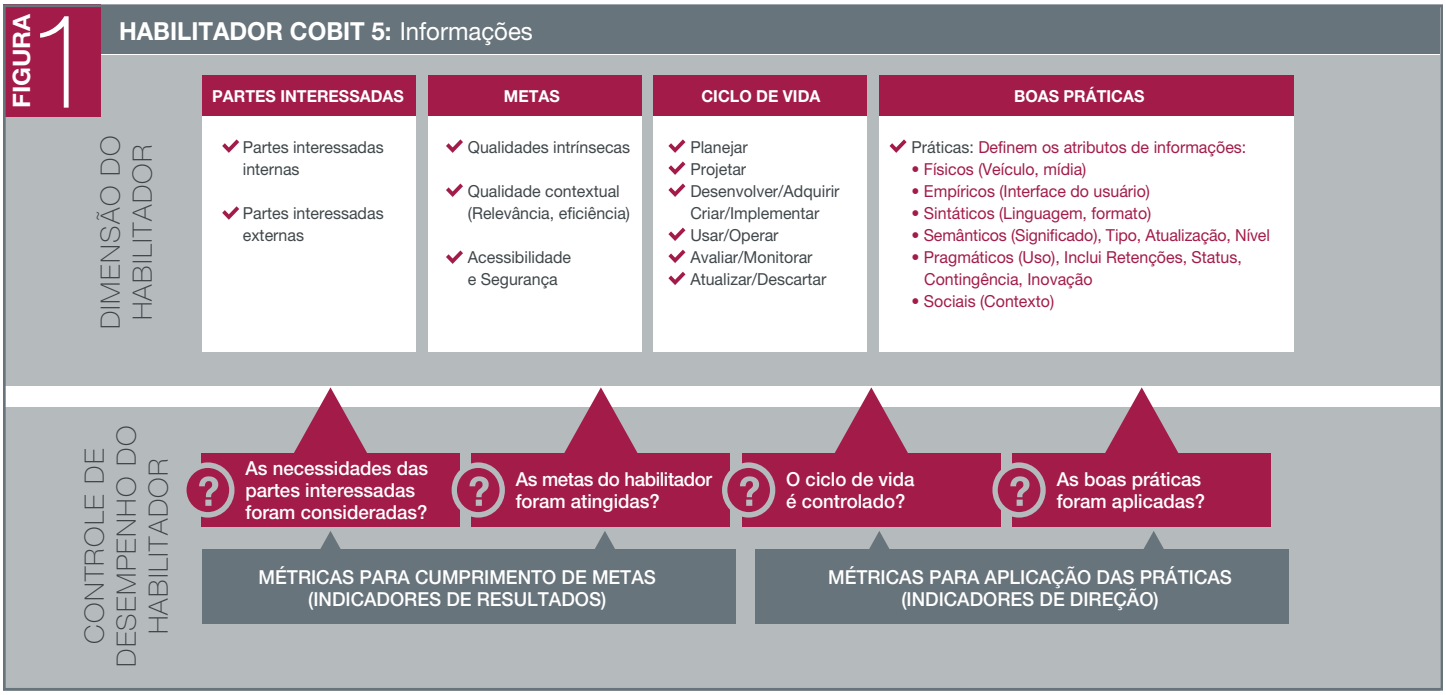
Lidar com dados desta magnitude diariamente e em tempo real apresenta uma nova fronteira e o nascimento de desafios de dados, incluindo:

- **Complexa evolução tecnológica;**
- **Integridade e privacidade de dados;**
- **Segurança dos dados em repouso e em movimento;**
- **Disponibilidade e resiliência do sistema de dados (infraestrutura de TI);**
- **Resposta a incidente e gerenciamento de violações de Big Data;**
- **Governança, risco e conformidade;**
- **Identidade e gerenciamento de acesso;**
- **Falta de habilidade neste domínio.**

Big Data é inerentemente vulnerável à violação de privacidade e dados, deixando iminente sua prevenção. Porém, fazer isso se tornou um desafio devido ao:

- **Aumento na complexidade do ambiente de TI;**
- **Crescimento massivo de volumes de dados de transação;**
- **Explosão dos novos tipos de dados de interação, como mídia social e dados do dispositivo;**
- **Uso de estrutura com base em java inseguro, como Apache™ Hadoop® e seu paradigma de programação MapReduce;**
- **Ameaças externas e internas;**
- **Ameaça persistente avançada (APT).**

Violações de dados na empresa são ocorrências comuns preocupantes que causam impacto nas empresas e agências do governo



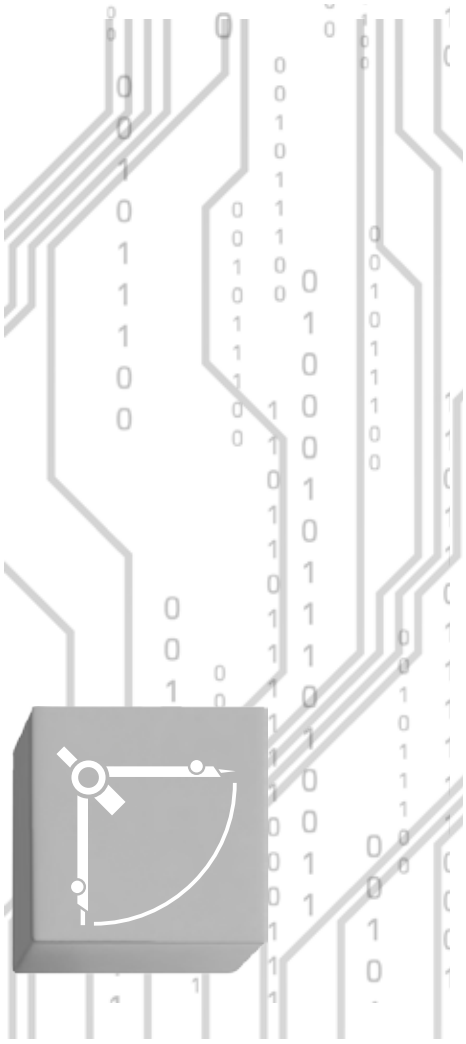
Fonte: COBIT® 5 para Segurança de Informação, ISACA, EUA, 2012, figura 16

diariamente. Além da publicidade negativa, essas violações, muitas vezes têm efeitos amplamente profundos sobre o negócio, incluindo os custos tais como multas regulatórias, taxas judiciais, honorários de consultoria e a perda de clientes. Como resultado, as empresas precisam mais e mais soluções de privacidade de dados robustos para evitar quebras e garantir a segurança de dados como mover dados de ponto a ponto e internacionalmente.

Conforme esses volumes de dados aumentam, essas novas estratégias precisam poder ser classificadas junto com eles. As empresas precisam de uma solução robusta de privacidade de dados para evitar violação e reforçar a segurança de dados em um ambiente complexo de TI. A solução deve reforçar as empresas ao:

- **Identificar todos os dados sensíveis;**
- **Garantir que os dados sensíveis estejam identificados e seguros;**
- **Demonstrar conformidade com todas as leis e regulamentações aplicáveis;**
- **Monitorar de modo proativo os dados e o ambiente de TI;**
- **Reagir e responder mais rápido às violações de privacidade e dados com gerenciamento de incidente.**

As fases do ciclo do habilitador de informação COBIT 5 (planejar, projetar, desenvolver/adquirir, usar/operar, monitorar e descartar), exibidas na **figura 1**, permitem que a empresa considere esses recursos de solução de privacidade e otimize a governança, a gestão de risco e a entrega efetiva dos projetos de implementação de Big Data.



Risco de Privacidade de Big Data

A análise preditiva de big data é uma extraordinária ferramenta quando usada e aplicada corretamente. A coleta de dados aparentemente não relacionados é inofensiva, mas seus poderes de previsão podem superar as expectativas. Por exemplo, o setor de saúde valoriza o Big Data como um indicador de comportamento de pacientes e a saúde futura. O serviço Google Now™ rastreia a localização do usuário do dispositivo móvel, eventos de calendário, pesquisa preferências pessoais e consultas. Este serviço prevê as necessidades de informação de um usuário e exibe as informações no dispositivo móvel do usuário. Usando os dados pessoais rastreados com o Google Now e as transações do cartão de pagamento, a análise preditiva do setor de saúde pode categorizar os estilos de vida do paciente como saudáveis ou não saudáveis. A análise preditiva pode categorizar um indivíduo incorretamente, com base em apenas um dos parâmetros rastreados. As empresas querem reduzir este tipo de risco com os filtros apropriados e verificações cruzadas.

O risco relacionado ao big data pode ser categorizado como operacional ou baseado na tecnologia da informação. Essas categorias de risco podem ser reduzidas com forte governança.

O risco operacional abrange os fatores internos e externos, que incluem risco geopolítico e a corrida para satisfazer a diretoria e a gerência sênior, que querem sair na frente da concorrência. O risco geopolítico, que é criado pelas políticas do país, inclui as leis da União Europeia, que restringem o processamento e compartilhamento transfronteiras, as leis de privacidade, que evitam a comercialização de certos grupos etários e as leis de privacidade dos EUA, que evitam a rotulação e compartilhamento de informações pessoais, privadas e financeiras, que podem levar a identificar roubos e transações não autorizadas. A legislação específica da indústria, como US HIPAA, pode ser bem complexa e os fornecimentos supondo transferências de risco podem não estar claramente documentados ou executados. “Os dados em si não criam valor ou causam problemas; seu uso sim.”[5]
Os CIOs corporativos podem ser pressionados pela diretoria ou gerência sênior para implementar o Big Data para poder competir antes que os controles de risco adequados sejam aplicados. Os controles de desenvolvimento de aplicação mal concebida podem levar a vazamento de dados e exposição de dados privados que não devem ser vistos pelos desenvolvedores.

Metodologias como Agile podem ser compatíveis com uma abordagem controlada do risco, permitindo flexibilidade. O mapeamento do Agile ao COBIT 5 pode ser uma abordagem adequada para governança, aquisição e desenvolvimento.

O risco de TI é também dos negócios - especificamente, o risco de negócios associado ao uso, titularidade, operação, envolvimento, influência e adoção de TI em uma empresa.[6] O risco de TI ocorre quando as garantias de segurança são superadas. Por exemplo, uma empresa pode adquirir as ferramentas de software, pois os tecnólogos consideram escalonáveis, mas não necessariamente, pois as ferramentas atendem às necessidades daqueles que planejam seu uso para análise comercial. As operações de TI podem ser tão focadas no desenvolvimento e entrega, que garantias de segurança simples para o planejamento da capacidade são ignoradas e os dados não são monitorados ou planejados corretamente.

As políticas empresariais precisam assegurar que os funcionários mantenham a confidencialidade das informações da parte interessada durante e depois do emprego. Este risco está aumentando, principalmente porque a informação se tornou a moeda do século XXI e os agentes de dados estão lucrando com a venda de informações - geralmente referentes aos dados como um serviço.

[5] *Op cit* Fórum Mundial Econômico, 2013
[6] ISACA.org, *The Risk IT Framework*, EUA, 2009, *www.isaca.org/Knowledge-Center/Research/Documents/RiskIT-FW-18Nov09-Research.pdf*

Estratégias de Privacidade de Big Data

Vários grupos estão começando a ver a necessidade de estabelecer normas para privacidade de Big Data. Um relatório do Fórum Mundial Econômico recomenda uma regulamentação que coloque restrições no uso de dados pessoais e no uso da tecnologia para fortalecer a privacidade individual. A privacidade pode ser embutida na tecnologia, assim os indivíduos têm controle sobre suas próprias informações.[7] O relatório sugere que os futuros sistemas de dados possam identificar todos os dados coletados com código que indica as preferências do indivíduo sobre como seus dados são usados.[8] A Associação da Indústria de Informação e Software (SIIA) avisa sobre a legislação da privacidade de Big Data e recomenda que as empresas tomem a iniciativa de criar a privacidade nas políticas de Big Data. O Diretor Sênior de SIIA, David LeDuc, expressou que as empresas podem se beneficiar do Big Data enquanto protegem a privacidade do usuário. Por exemplo, ele recomenda ocultar os dados do cliente o mais rápido possível. Ocultar permanentemente remove os identificadores pessoais dos dados. A SIIA e outros grupos industriais gostariam de ver organizadores de políticas, defensores do consumidor e outras partes interessadas se juntarem para criar a política.[9]

Ao entender as tendências globais na gestão de privacidade, as organizações podem determinar uma estratégia defensiva ou ofensiva para a privacidade de Big Data. Uma estratégia defensiva inclui adotar a capacidade de usar informações e proteger a privacidade de indivíduos por várias formas de resumir e identificar. A ocultação pode dar suporte à tendência estatística e análise e suporte da privacidade individual, quando necessário. Uma estratégia ofensiva envolve forçar a revelação e lembrar o consumidor da troca de serviços e dados. Por exemplo, esta estratégia seria implementada para serviços que obtenham informações pessoais em troca de emitir cupons, trocando serviços gratuitos, permuta de produtos como assinaturas gratuitas de revistas, flores grátis, e-mail grátis ou serviços de agenda.

Governança da Privacidade de Big Data

Big Data dá às empresas a capacidade de acessar, agregar e analisar a sempre crescente quantidade de dados, incluindo páginas Web, hábitos de navegação, sinais de sensor, rastreamento de local de smartphone e informações genéricas. Big Data é uma enorme oportunidade para fazer a informação o líder da criação de valor, mas sem compreensão dos princípios, políticas e estruturas, o Big Data pode gerar enorme risco. O Big Data precisa de uma plataforma de governança que garanta confiabilidade na melhor utilização dos dados.

Sem a governança adequada, os mesmos dados que podem ser usados para criar valor, podem ser usados para criar resultados intrusos e prejudiciais e tomada de decisão destrutiva.

COBIT 5 permite que as empresas criem valor ideal de TI ao manter o equilíbrio entre realizar benefícios e otimizar os níveis de risco e recursos.

[7] *Op cit* Fórum Mundial Econômico, 2013

[8] Lohr, Steve, "Big Data Is Opening Doors, but Maybe Too Many", *The New York Times*, 23 de março de 2013, *www.nytimes.com/2013/03/24/technology/big-data-and-a-renewed-debate-over-privacy.html?_r=1&*

[9] Associação de Informação da Indústria e Software, "Inovação Impulsionada pelos Dados: Um guia para decisores: Entender e facilitar o valor socioeconômico dos dados", maio de 2013, *www.siia.net*

Empresas existem para criar valor para suas partes interessadas, enquanto otimizam o risco e o uso de recursos. Oferecer valor à parte interessada da empresa necessita de boa governança e gerenciamento de informações e ativos de TI. Big Data é um ativo da empresa que se ajusta naturalmente no domínio do Princípio 1 de COBIT 5 - Atender às Necessidades da Parte Interessada.

COBIT 5 faz uma diferenciação clara entre governança e gerenciamento, com a responsabilidade da governança em nível de diretoria. As necessidades da parte interessada do Big Data são asseguradas e mantidas em um alto nível na empresa. A Tabela RACI COBIT5 para um dos processos de governança corporativa, na **figura 2**, mostra que a diretoria é responsável pelas iniciativas críticas, enquanto a responsabilidade de gerenciamento está com o Chief Executive Officer (CEO) e o CIO. A tabela RACI atribui os níveis de responsabilidade para as práticas do processo para funções e estruturas. As funções da empresa estão em vermelho e as de TI, em azul. Os diferentes níveis de envolvimento são:

R (Responsável) - Participar da operação principal em atender a atividade listada e criando o resultado pretendido;

A (Responsabilizado) - é responsável pelo sucesso da tarefa;

C (Consultado) - oferece resultado;

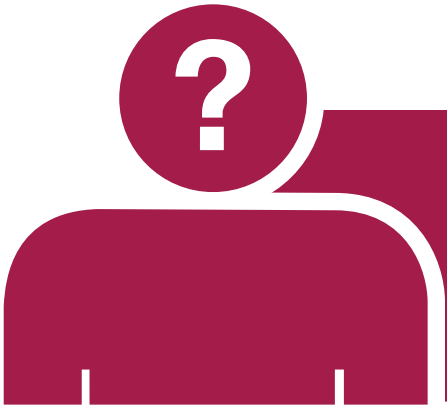
I (Informado) - recebe informações sobre as conquistas e/ou resultados da tarefa;

FIGURA 2 **COBIT 5 EDM01:**
Garantir o Ajuste da Estrutura de Governança e Manutenção do Processo de Atribuição de Função

Tabela EDM01 RACI

Fonte: COBIT® 5: Processos de Habilitação, ISACA, EUA, 2012, pág. 31

EDM01.03 Monitorar o Sistema de Governança	EDM01.02 Direcionar o Sistema de Governança	EDM01.01 Avaliar o Sistema de Governança	PRINCIPAIS PRÁTICAS DE GOVERNANÇA
A	A	A	Diretoria
R	R	R	Chief Executive Officer
C	C	C	Chief Financial Officer
C	C	C	Chief Operating Officer
R	R	R	Executivos de Negócios
I	I		Proprietários de Processos de Negócios
R	R	R	Comitê Executivo de Estratégia
I	I		Comitê de Direção (Programas/Projetos)
I	I		Escritório de Gestão de Projetos
I	I		Escritório da Gestão de Valor
C	C	C	Chief Risk Officer
I	I		Chief Information Security Officer
I	I	C	Diretoria de Arquitetura
I	I	C	Comitê de Risco Empresarial
I	I	C	Recursos Humanos de Diretoria
C	C	C	Conformidade
C	C	C	Auditoria
R	R	R	Chief Information Officer
C	C	C	Gestor de Arquitetura
I	I	C	Líder de Desenvolvimento
I	I	C	Gestor das Operações de TI
I	I		Gestor da Administração de TI
I	I		Gerente de Serviço
I	I		Gerente de Segurança da Informação
I	I		Gerente da Continuidade dos Negócios
I	I		Privacy Officer



Para a governança adequada da privacidade de Big Data, a diretoria e os executivos sêniores devem fazer as seguintes perguntas:

A diretoria e os executivos sêniores devem aceitar TI com liderança que assegure as políticas corretas, processos e procedimentos e um conjunto de habilidades apropriados.

A privacidade em uma empresa inclui conformidade com as exigências jurídicas e regulatórias sobre os períodos de retenção de dados, regulamentação internacional, privacidade e propriedade intelectual (PI). A governança de privacidade de Big Data deve garantir a conformidade, mas, ao mesmo tempo, permitir um ambiente corporativo que use efetivamente o Big Data para criar concorrência sustentável.

- Quais princípios, políticas e estruturas vamos estabelecer para dar suporte à conquista de estratégia comercial pelo Big Data?
- Podemos confiar em nossas fontes de Big Data?
- Quais estruturas e habilidades temos para governar e gerenciar TI?
- Quais estruturas e habilidades temos para governar privacidade de Big Data?
- Temos as ferramentas corretas para atender nossas especificações de privacidade de Big Data?
- Como verificamos a autenticidade dos dados?
- Podemos verificar como a informação será usada?
- Quais opções de decisão temos com relação à privacidade de Big Data?
- Qual é o contexto para cada decisão?
- Podemos simular as decisões e entender as consequências?
- Vamos registrar as consequências e usar essa informação para fornecer nosso processo de coleta de informação de Big Data, contexto, análise e tomada de decisão?
- Como vamos proteger nossas fontes, nossos processos e nossas decisões contra roubo e corrupção?
- Estamos explorando as ideias que temos do Big Data?
- Quais informações estamos coletando sem expor a empresa a disputas jurídicas e regulatórias?
- Quais ações estamos tomando que criam tendências que podem ser exploradas por nossos rivais?
- Quais políticas estão em vigor para garantir que os empregados mantenham a confidencialidade das informações da parte interessada durante e depois da admissão?

Considerações de garantia para privacidade de Big Data

Os principais drivers para segurança incluem:

- **Oferecer às partes interessadas as opiniões substanciais sobre governança e gerenciamento de TI corporativa, de acordo com os objetivos de segurança;**
- **Definir os objetivos de segurança alinhados com os objetivos da empresa, maximizando assim o valor das iniciativas de segurança;**
- **Satisfazer as especificações contratuais e regulatórias para empresas, para oferecer segurança sobre as organizações de TI.**

Os profissionais de segurança devem ser parte da iniciativa de Big Data corporativa desde o início. Para poder oferecer ideias valiosas de Big Data para a empresa, os profissionais de segurança precisam ter entendimento profundo dos negócios; o conhecimento, como cientistas de dados, para usar ferramentas de Big Data, como Hadoop, a plataforma EMC® Greenplum®, o software de banco de dados Teradata® e aplicações analíticas, sistema analítico HP™ Vertica™ e software Palantir Technologies; e as habilidades para interpretar os resultados e explicá-los corretamente às partes interessadas. Os profissionais de segurança devem se manter bem informados sobre as novas habilidades e termos de Big Data e educar a equipe de auditoria e gerenciamento.

Além de oferecer ideias de Big Data para gerenciamento, os profissionais de segurança devem atestar que:

- **As soluções de segurança e privacidade de Big Data sejam implementadas;**
- **Exista governança suficiente de privacidade de Big Data, como:**
  - Data anonymization/sanitization ou de-identification;
  - Políticas de privacidade de Big Data, processos, procedimentos e estrutura de suporte atuais, úteis, relevantes e adequados;
  - Apoio ao gerenciamento sênior e evidência de comprometimento contínuo;
  - Destruição de dados apropriados, política de gestão de dados ampla, titularidade e responsabilidade de eliminação claramente definidas;
  - Conformidade com especificações de dados jurídicas e regulatórias;
  - Educação contínua e treinamento das políticas de Big Data, processos e procedimentos.

Conclusão

O Big Data está se tornando cada vez mais difundido e as empresas precisam descobrir as maneiras ideais de obter seus benefícios. A privacidade é uma área que exige muita atenção, já que o Big Data está centralizado de modo inerente no indivíduo. A dependência tem o potencial de criar consequências negativas significativas.

Big Data é um ativo valioso e, ao mesmo tempo, uma ferramenta poderosa com impactos bem vastos. Como consequência, as iniciativas de Big Data precisam ter visibilidade para a diretoria e patrocinadores de nível executivo.

O sucesso das empresas vai depender de como elas atendem e lidam com os vários desafios de Big Data e os seus impactos, incluindo a privacidade. **Para aproveitar valor e soluções analíticas mais rápidas e resilientes à oferta, as empresas devem implementar soluções de Big Data usando estruturas e processos bem definidos, juntamente com uma boa governança e estrutura de gerenciamento de risco.**