INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS

BACHARELADO EM SISTEMAS DA INFORMAÇÃO

ELEMENTOS DE PREVENÇÃO DO APRISIONAMENTO TECNOLÓGICO

GUILHERME ALVES DE OLIVEIRA

GOIÂNIA
2021

INSTITUTO FEDERAL
Goiás

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
SISTEMA INTEGRADO DE BIBLIOTECAS

TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO NO REPOSITÓRIO DIGITAL DO IFG - ReDi IFG

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia de Goiás, a disponibilizar gratuitamente o documento no Repositório Digital (ReDi IFG), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IFG.

Identificação da Produção Técnico-Científica

[ ] Tese	[ ] Artigo Científico
[ ] Dissertação	[ ] Capítulo de Livro
[ ] Monografia – Especialização	[ ] Livro
[X] TCC - Graduação	[ ] Trabalho Apresentado em Evento
[ ] Produto Técnico e Educacional - Tipo: _____	

Nome Completo do Autor:
Matrícula:
Título do Trabalho:

Autorização - Marque uma das opções

1. (X) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso aberto);
2. ( ) Autorizo disponibilizar meu trabalho no Repositório Digital do IFG somente após a data ___/___/_____ (Embargo);
3. ( ) Não autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso restrito).

Ao indicar a opção **2 ou 3**, marque a justificativa:

( ) O documento está sujeito a registro de patente.
( ) O documento pode vir a ser publicado como livro, capítulo de livro ou artigo.
( ) Outra justificativa: _____

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

i. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
ii. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia de Goiás os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
iii. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

Goiânia, 14/03/22.
Local Data

Guilherme Alves de Oliveira
Assinatura do Autor e/ou Detentor dos Direitos Autorais

GUILHERME ALVES DE OLIVEIRA

ELEMENTOS DE PREVENÇÃO DO APRISIONAMENTO TECNOLÓGICO

Trabalho de Conclusão de Curso apresentado no Instituto Federal de Educação, Ciência e Tecnologia de Goiás como requisito básico para a conclusão do Curso de Sistemas de Informação.

Orientador(a): Me. Carina Calixto Ribeiro de Araújo
Coorientador: Me. Ariel Cardoso Mendes

GOIÂNIA

2021

O48 Oliveira, Guilherme Alves de.
Elementos de prevenção do aprisionamento tecnológico / Guilherme Alves de Oliveira. – Goiânia : Instituto Federal de Educação, Ciência e Tecnologia de Goiás, 2021.
48f.

Orientação: Me. Carina Calixto Ribeiro de Araújo.
Coorientação: Me. Ariel Cardoso Mendes.

TCC (Trabalho de Conclusão de Curso) – Curso de Bacharelado em Sistemas de Informação, Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

1. Governança de TI. 2. Aprisionamento tecnológico. I. Araújo, Carina Ribeiro de (orientação). II. Mendes, Ariel Cardoso (coorientação). III. Instituto Federal de Educação, Ciência e Tecnologia de Goiás. IV. Título.

CDD 658.403 8

Ficha catalográfica elaborada pela bibliotecária Lana Cristina Dias Oliveira CRB1/ 2.631
Biblioteca Professor Jorge Félix de Souza,
Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Goiânia.

ATA DA SESSÃO PÚBLICA DE APRESENTAÇÃO E

DEFESA DO TRABALHO DE CONCLUSÃO DE CURSO

AOS DEZ DIAS DO MÊS DE FEVEREIRO DE DOIS MIL E VINTE E DOIS, A PARTIR DAS DEZENOVE HORAS, NA SALA DE VIDEOCONFERÊNCIA GOOGLE MEETS REALIZOU-SE A SESSÃO DE DEFESA DO TRABALHO DE CONCLUSÃO DE CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO INTITULADO: A GOVERNANÇA COMO UM ELEMENTO DE PREVENÇÃO DO APRISIONAMENTO TECNOLÓGICO, DE AUTORIA DO DISCENTE GUILHERME ALVES DE OLIVEIRA, SOB ORIENTAÇÃO DA PROFESSOR(A) CARINA CALIXTO RIBEIRO DE ARAUJO E CO-ORIENTAÇÃO DO PROFESSOR ARIEL CARDOSO MENDES DE ACORDO COM OS CRITÉRIOS DESCRITOS NA RESOLUÇÃO IFG N° 028, DE 11 DE AGOSTO DE 2014, AS NOTAS FORAM ATRIBUÍDAS PELOS COMPONENTES DA BANCA EXAMINADORA, SENDO O TRABALHO AVALIADO COM O SEGUINTE CONCEITO: NOTA 6,0 - APROVADO COM CORREÇÕES. A BANCA CONCEDEU O PRAZO DE 30 DIAS PARA A REALIZAÇÃO DAS CORREÇÕES APONTADAS.

_____

Prof. Me. Carina Calixto Ribeiro - Orientadora - DAAIV - IFG/Goiânia

_____

Prof. Me. Ariel Cardoso Mendes - Co-Orientador - DAAIV - IFG/Goiânia

_____

Prof. Me. Dory Gonzaga Rodrigues - DAAIV - IFG/Goiânia

_____

Prof. Esp. Douglas Rolins de Santana - DAAIV - IFG/Goiânia

Documento assinado eletronicamente por:

- **Carina Calixto Ribeiro de Araujo**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 15/03/2022 09:35:16.
- **Douglas Rolins de Santana**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 14/03/2022 14:33:51.
- **Dory Gonzaga Rodrigues**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 14/03/2022 14:02:08.
- **Ariel Cardoso Mendes**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 14/03/2022 13:51:29.

Este documento foi emitido pelo SUAP em 14/03/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifg.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 256837
Código de Autenticação: 831674fa17

GUILHERME ALVES DE OLIVEIRA

ELEMENTOS DE PREVENÇÃO DO APRISIONAMENTO TECNOLÓGICO

Trabalho de Conclusão de Curso apresentado no Instituto Federal de Educação, Ciência e Tecnologia de Goiás como requisito básico para a conclusão do Curso de Sistemas de Informação.
Orientador(a): Carina Calixto Ribeiro de Araújo
Coorientador: Ariel Cardoso Mendes

Aprovada em de de

BANCA EXAMINADORA

Prof. Me. Carina Calixto Ribeiro - Orientadora
Coordenação de Informática/DAAIV/IFG - Campus Goiânia

Prof. Me. Ariel Cardoso Mendes - Co-Orientador
Coordenação de Informática/DAAIV/IFG - Campus Goiânia

Prof. Me. Dory Gonzaga Rodrigues
Coordenação de Informática/DAAIV/IFG - Campus Goiânia

Prof. Esp. Douglas Rolins De Santana
Coordenação de Informática/DAAIV/IFG - Campus Goiânia

GOIÂNIA

2021

AGRADECIMENTOS

Dedico nesta página uma homenagem a todos os envolvidos na concretização deste sonho. Agradeço, primeiramente, às minhas avós Eliana e Elizabete que me deram os motivos, as lições de moral e o suporte necessário para a continuar e persistir na minha jornada acadêmica, inclusive na escrita deste trabalho, agradeço aos meus pais pelos exemplos que demonstram que a vida de estudante não é fácil, mas é um caminho digno e honesto para ser seguido.

Agradeço ao IFG e a todos os professores que fizeram o seu melhor para ensinar e não para cobrar e julgar.

Agradeço à minha orientadora, Carina Calixto e meu coorientador Ariel pelo voto de confiança no trabalho e pelo apoio e envolvimento no mesmo. Aos colegas e amigos que encontrei e que colaboraram comigo na faculdade. Agradeço aos demais profissionais do IFG que deram suporte para a conclusão do curso, aos meus amigos e colegas da área que me incentivaram e deram perspectivas para enfrentar essa jornada. E a todos os outros que se dedicaram em prol do curso de bacharelado em Sistemas de Informação.

“Em três anos, todos os produtos da minha companhia estarão obsoletos. A única pergunta é se somos nós mesmos os que vão deixá-los obsoletos ou se outra pessoa fará isso primeiro.”

Bill Gates

SUMÁRIO

LISTA DE TABELAS E ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANSI	*American National Standards Institute*
API	*Application Programming Interface*
COBIT	*Control Objectives for Information and Related Technology*
CSC	*Cloud Service Customer*
CSN	*Cloud Service Partner*
CSP	*Cloud Service Provider*
DIS	*Draft International Standard*
DP	*Draft Proposal*
DTP	*Data Transfer Poject*
GC	Governança Corporativa
GTI	Governança de TI
HTML	*HyperText Markup Language*
IBM	*International Business Machines*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Eletrical and Electronicas Engineers*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
OASIS	*Organization for the Advancement of Structured Information Standards*
PC	*Personal Computer*
SQL	*Structured Query Language*
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
W3C	*World Wide Web Consortium*

RESUMO

Não se pode negar a importância da informação para as organizações. A Tecnologia da Informação é um conjunto de atividades e soluções providas por recursos de computação que permitem gerar e tratar informações e automatizar os processos existentes, e assim funcionam como um facilitador de mudanças organizacionais que podem levar a ganhos adicionais de produtividade. As empresas precisam ter eficiência, disponibilidade, confiabilidade e o controle de suas informações, possibilitando a agilidade na análise dos dados para auxiliar nas decisões estratégicas. Na prática, isso acontece por meio de uma infraestrutura computacional própria ou terceirizada e com uso dos sistemas de informação. Se tornar dependente de uma marca de equipamentos ou de um fornecedor de serviços e/ou produtos de tal forma que fique extremamente difícil ou praticamente impossível trocar, é um risco que coloca a viabilidade econômica ou as informações da empresa em grande vulnerabilidade. Com o conceito de governança de TI amadurecido e a crescente necessidade das empresas em adotarem padrões que lhes permita maior previsibilidade de riscos, mais transparência nos controles da informação e no próprio uso da tecnologia, alguns modelos se popularizaram pelo seu auxílio na implementação da Governança de TI (GTI). Este estudo pretende analisar como boas práticas de governança e gerenciamento de serviços de TI podem ajudar a prevenir o aprisionamento tecnológico, também conhecido como *technology lock-in*.

Palavras-chave: Governança de TI, COBIT, ITIL, Aprisionamento tecnológico

ABSTRACT

The importance of information for organizations cannot be denied. Information Technology is a set of activities and solutions provided by computing resources that allow generating and processing information and automating existing processes, thus functioning as a facilitator of organizational changes that can lead to additional productivity gains. Companies need to have efficiency, availability, reliability and control of their information, enabling agility in data analysis to assist in strategic decisions. In practice, this happens through its own or outsourced computing infrastructure and using information systems. Becoming dependent on a brand of equipment or a supplier of services and/or products in such a way that it is extremely difficult or practically impossible to change, is a risk that puts the economic viability or the company's information in great vulnerability. With the concept of IT governance matured and the growing need for companies to adopt standards that allow them greater predictability of risks, more transparency in information controls and in the very use of technology, some models have become popular for their assistance in the implementation of IT (GTI). This study aims to analyze how good governance and management practices for IT services can help prevent aprisionamento tecnológico, also known as technology lock-in.

Keywords: IT Governance, COBIT, ITIL, technology lock-in

1. INTRODUÇÃO

A sociedade vem se adaptando cada vez mais às mudanças decorrentes dos avanços tecnológicos, especificamente no quesito da facilidade que é se informar e compartilhar a informação.

A dependência das pessoas e das instituições aos meios digitais de informação já é uma realidade em uma boa parte do mundo, seja para se entreter, para ganhar produtividade podemos afirmar com segurança que a tecnologia da informação está cada vez mais intrínseca na vida das pessoas.

A crescente dependência da humanidade em relação a soluções de tecnologia, em conjunto com o crescente e acelerado desenvolvimento da área da tecnologia da informação, acentuou a concorrência tecnológica nas suas mais diversas formas. Com isso surge a cada momento uma grande variedade de produtos dentro de um mesmo segmento, cada qual com suas propostas de solução para um determinado problema, seu diferencial de implementação/utilização e suas normas específicas e proprietárias, sem a devida preocupação de integração destas soluções distintas.

O crescimento acelerado de TI trouxe muito desenvolvimento, mas pelo ritmo acelerado que os hardwares e softwares se desenvolveram e se tornaram acessíveis, as possibilidades do que fazer com essa tecnologia também se desenvolveram, mais produtos foram sendo disponibilizados no mercado de tecnologia, com isso, algumas dessas soluções sem a devida padronização e/ou regulamentação nas formas de oferecer os serviços de tecnologia acabam se tornando um problema mais adiante.

Alguns vestígios da falta de uma padronização em alguns serviços de tecnologia da informação são evidenciados nos momentos em que um software de uma marca não podem ser aproveitados em equipamentos de outra ou em que existem formatos diferentes de arquivos com a mesma funcionalidade, tendo a diferença de que alguns deles só abrem em softwares específicos e se tentarmos fazer um conversão podemos ter desde perda de qualidade, formatação e até de informação, obrigando os clientes em razão desta situação a permanecer com a solução já em uso, mesmo que haja algum tipo de perda ou custo adicional para sua

manutenção. Esse fenômeno configura o que denominamos “aprisionamento tecnológico” que em inglês é denominado *technology lock-in*.

Neste trabalho iremos analisar o assunto com o apoio das boas práticas de governança de TI, buscando identificar meios de prevenção para que tal problema não assombre instituições causando-lhes dependência de tecnologias muito específicas. Esta situação pode vir a causar diversos outros problemas para estas instituições tais como o alto custo de troca, de manutenção ou de migração, podendo até mesmo colocar a empresa em risco.

Sabemos que isso já aconteceu no passado, quando as tecnologias proprietárias dominavam o ambiente computacional como por exemplo, uma empresa que operasse um mainframe IBM não conseguiria expandir seu parque de terminais com equipamentos Unisys nem vice-versa, cada um com sua tecnologia proprietária de conexão. Situações como esta levaram à necessidade de definições de padrões que fossem adotados por toda indústria, mas ainda hoje com a forte evolução tecnológica e a oferta cada vez mais intensa de serviços de tecnologia esta situação ainda persiste e deve ser uma preocupação para as organizações de qualquer porte. Portanto, onde os esforços de padronização não alcançam é necessário estar atento e preparado para se evitar o risco de aprisionamento.

Conforme as informações em uma organização são geradas, surgem novas estratégias necessárias para o aumento de competitividade e o alcance dos objetivos que a instituição se propõe. Estas organizações vêm fazendo uso cada vez mais intenso da tecnologia como suporte de negócios.

Em vista dessa realidade da TI, a adequada administração, planejamento e controle sobre a utilização dos recursos de TI ganha cada vez mais valor, impactando no cuidado com a informação para auxílio nas estratégias definidas e até mesmo para a sobrevivência das organizações. Nessas circunstâncias, evitar o aprisionamento tecnológico pode ser um grande investimento, ou melhor, uma grande economia.

2. REFERENCIAL TEÓRICO

2.1. Aprisionamento tecnológico

Segundo Cerqueira (2017) o aprisionamento tecnológico é uma estratégia comercial moralmente questionável. Consiste na criação de uma dependência do consumidor em relação ao fornecedor. Essa dependência costuma vir acompanhada de altos custos, relacionados geralmente a reparos, atualizações e melhorias. Em resumo, é uma relação parasitária.

> Quando a informação é armazenada de forma que seja acessível somente por um produto específico, o dono desta informação fica refém do fornecedor deste produto para continuar tendo acesso às próprias informações (CERQUEIRA, 2017, p. 2).

Às vezes empresas de TI adotam estratégias fazendo com que seus clientes se tornem dependentes de seus produtos ou serviços de tal forma que fica impossível ou inviável uma rescisão de contrato ou trocar a marca do produto sem acarretar grandes danos para o cliente, e juntando ao fato de que quanto mais a sociedade adota uma determinada tecnologia, menos provável é que os usuários mudem. Surge então o problema do aprisionamento tecnológico ou *technology lock-in*.

Para Cerqueira (2017) o aprisionamento tecnológico é especialmente crítico quando se lida com informações. A maneira que se escolhe para armazenar informações deve ser feita com muito cuidado, pois à medida que o tempo passa, a quantidade de informações armazenadas tende a aumentar. Isso significa que os custos de uma possível migração no futuro também vão aumentar.

> A perda de informações pode significar a ruína de todo um negócio, ou ao menos um grande prejuízo. Muitos fornecedores de produtos ou serviços relacionados à tecnologia da informação se aproveitam disso. Quando a informação é armazenada de forma que seja acessível somente por um produto específico, o dono desta informação fica refém do fornecedor deste produto para continuar tendo acesso às próprias informações (CERQUEIRA, 2017, p. 2).

O que acontece se uma organização precisar mudar de fornecedor? Há inúmeros motivos que podem ser elencados para justificar uma possível necessidade de migração. Alguns exemplos são:

- ✓ O fabricante/provedor do serviço pode ter ido à falência;
- ✓ O custo do serviço/licença pode se tornar inviável;
- ✓ Uma tecnologia mais aderente às suas necessidades pode surgir;
- ✓ O provedor do serviço pode definir novas políticas/termos de uso, com os quais o cliente não concorde;
- ✓ O serviço ou produto pode depender de tecnologias que não são mais viáveis dentro da sua infraestrutura.

Então é importante ter sempre um plano B, isto é, estar preparado para eventuais necessidades de migrações no futuro. Bons gestores sabem quanto tempo, esforço e dinheiro isso pode poupar (e bons técnicos sabem quão oneroso e desgastante tecnicamente pode ser este processo). E essa regra vale para tecnologias domésticas ou pessoais também, não apenas dentro de empresas. Acontece que certos serviços e tecnologias acabam criando uma bolha da qual é difícil se desvencilhar, o que inviabiliza uma possível migração. Essa estratégia é vantajosa apenas para o provedor do serviço, mas pode se tornar um grande problema para o cliente (CERQUEIRA, 2017, p. 2-3).

> Numa visão econômica, o aprisionamento do conteúdo, do aplicativo e do equipamento, pode apresentar a maximização de resultado, aplicação dada pela *Apple*, empresa que idealiza e comercializa produtos eletrônicos de consumo. Ou seja, “a *Apple* se recusa a licenciar seu sistema operacional […]. Se você quer uma impressora a *laser*, *software*, ou qualquer acessório virtual, você deve possuir um da Apple”. Esse é um exemplo de *lock-in*(WU, 2010, p. 291).

A Web facilita a interação entre usuários, mas, simultaneamente, algumas empresas de tecnologia procuram limitar o acesso à informação e aprisionar o consumidor, principalmente por questões econômicas (CARVALHO; PEREIRA; VERGIL, 2012, p. 8).

Em seu trabalho denominado a Economia da Informação, Shapiro e Varian (1999) apresentam o ciclo de aprisionamento através da figura que reproduzimos abaixo.

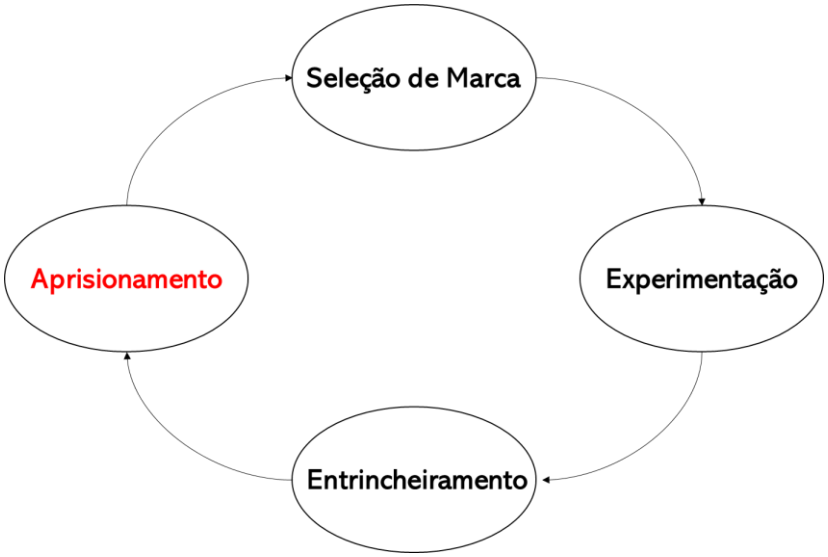

Figura 1. Ciclo de aprisionamento.
Fonte: Adaptado de Shapiro e Varian (1999).

A abordagem entende que o aprisionamento pode começar ao se selecionar a marca de um produto ou serviço a partir do momento em que com sua escolha, por suas características, se reduz a possibilidade de mover para uma outra marca. Na sequência vem a experimentação na qual se usufrui das vantagens e dos benefícios que ela provê. Na fase do entrincheiramento o usuário se acostuma com a nova marca passando a dar preferência a mesma em detrimento de outras podendo incorrer com o decorrer do tempo em maior custo para a troca da solução. Na sequência se adentra na fase do aprisionamento deste em que os custos, não só financeiros, se tornam mais altos para a troca de fornecedor.

Shapiro e Varian (1999) definem que os custos de troca medem a extensão do aprisionamento do consumidor a um determinado fornecedor. Em muitos casos, a possibilidade de interrupção no serviço que pode ocorrer em consequência da troca de fornecedores é uma consideração importante a ser feita para se decidir pela troca (saída do aprisionamento) ou não.

Definem ainda que, quando o custo de mudar de uma marca ou tecnologia para outra é significativo, o usuário da solução tecnológica está enfrentando o aprisionamento. Assim, ao adquirir soluções de TI, é essencial ter uma noção ampla dos custos de troca futuros.

O que chamamos de soluções de TI neste trabalho é qualquer recurso de hardware ou software isolado, ou mesmo a conjugação dos dois, associados a

tecnologias de comunicação e outros serviços de tecnologia da informação que fornecem à organização a possibilidade de automatizar, racionalizar suas atividades. Por esta definição um serviço de computação em nuvem é uma solução de TI, ao mesmo tempo em que um sistema instalado em um armazém composto de sensores de RFID, aplicação servidora na retaguarda com servidor(es) físico(s) com seu hardware e sistema operacional específico, seu respectivo sistema de controle e mais um sistema gerenciador de banco de dados comporiam uma solução de TI.

Em sua abordagem, Shapiro e Varian defendem que para uma empresa diminuir seu aprisionamento a uma solução ela precisa ser capaz de visualizar os desdobramentos futuros para poder traçar uma estratégia que reduza a dependência de determinada solução.

2.1.1 O impacto do aprisionamento

Não se pode negar a importância da informação para as organizações. A diferença da informação para os ativos tangíveis convencionais é a sua dificuldade de administração e avaliação. E assim, em um cenário cada vez mais competitivo, a busca incessante por informações tem dado alternativas para as organizações se adaptarem ao panorama de mudanças constituídas pela demanda crescente por novas tecnologias de informação (CHIMENDES; NEVES, 2010, p. 4).

Nos tempos atuais é de suma importância que as informações estejam disponíveis, de forma atualizada, precisa com qualidade e segurança, pois informação perdida é poder competitivo e estratégico perdido e são gráficos com menos dados para tomadas de decisão.

Ao implementarem programas de mudança para melhor cumprir seus objetivos, as organizações podem se deparar com a necessidade de alterar estruturas, processos internos e tecnologias.

> Em função da grande presença de tecnologias nos processos de negócio atuais, frequentemente as necessidades de mudança envolvem decisões sobre as soluções de tecnologia de informação (TI) utilizadas, incluindo equipamentos (hardware), sistemas (software) e serviços (ENGELBERT; GRAEML, 2011, p. 159).

Nesse contexto, acaba sendo necessário comprar, aperfeiçoar, adaptar, desenvolver ou trocar a solução de TI existente e em uso pela organização por algo

novo. No caso de considerar a substituição da solução atual, a organização tem de levar em conta os eventuais custos de troca, que podem também ser trabalhosos e muito demorados.

Shapiro e Varian (1999) exemplificam alguns casos de aprisionamento ocorridos no passado, que vão desde casos envolvendo bilhões de dólares como o da operadora de telecomunicações americana Bell Atlantic que na década de 1980 investiu 3 bilhões de dólares em um parque de comutadores digitais telefônicos modelo 5ESS de fabricação da empresa americana AT&T que empregavam neste modelo de equipamento um sistema operacional proprietário controlado pela fabricante. O problema era que toda vez que a Bell Atlantic queria acrescentar uma nova capacidade, ou conectar esses comutadores a um novo equipamento periférico de hardware, dependia da AT&T para o fornecimento dos aprimoramentos necessários para o sistema adicional e o desenvolvimento das interfaces.

Uma outra situação da época da publicação de seu livro citada pelos autores, envolvendo valores menores (que também podem variar para mais ou menos dependendo do tamanho do parque computacional envolvido) mas bastante representativo da situação de aprisionamento, eram situações que envolviam os computadores Mac da Apple: “Você tem muito software para Mac, está familiarizado com a forma de usar o Mac, sua impressora Mac pode ainda lhe prestar alguns anos de bons serviços e você provavelmente troca arquivos com outros usuários do Mac. Você enfrentará custos significativos se decidir mudar de uma tecnologia de informação para outra.”

Neste exemplo envolvendo o computador Mac, o aprisionamento se apresenta sob diversas formas: pela familiaridade do usuário com o uso e a dificuldade, e a até mesmo a resistência, em mudar a forma de fazer as coisas que o usuário já se acostumou (nova curva de aprendizado – podendo refletir em baixa produtividade inicial no novo equipamento), no investimento que já foi feito em uma impressora compatível com o Mac que (a época) poderia não ser com o novo computador, a eventual necessidade e dificuldade de conversão de arquivos quando do intercâmbio de informações com outros usuários Mac quando já em utilização do novo modelo de computador. É a todo este cenário que os autores se referem como “custos significativos de mudar de tecnologia”. Se a situação se aplica não a um único usuário final, mas a uma organização inteira com vários desses equipamentos

em seu parque computacional, multiplica-se esta mesma situação pela quantidade de usuários e ainda pode ter que ser agregado uma nova questão, a da resistência à mudança por parte destes usuários rejeitando o novo equipamento e fazendo a produtividade cair mais ainda.

Como se pode perceber o aprisionamento não está limitado somente a grandes transações nem somente ao ambiente corporativo, ele pode se dar também no âmbito da pessoa física, o usuário final de qualquer produto ou serviço tecnológico.

Mesmo com a forte evolução tecnológica da época da publicação deste texto por parte dos seus autores para os dias atuais, os casos de aprisionamento ainda persistem nas relações clientes/fornecedores, tanto que alguns padrões publicados recentemente sobre tecnologias modernas por órgãos normatizadores internacionais se referem diretamente a este tema em seu teor.

A linha que define se um caso é ou não é aprisionamento tecnológico e passível de discussões às vezes até jurídica dependendo da cultura e conceitos de moral e ética de cada uma delas, casos recentes são os processos judiciais em 2021 onde o consumidor foi indenizado no Brasil porque o último smartphone da Apple veio sem o carregador.

Alguns outros casos em que o aprisionamento tecnológico pode se ver presente em algum nível e algumas questões que nos rodeiam são:

- Muitas pessoas não mudam o seu aplicativo de streaming de música simplesmente porque não querem criar a sua playlist novamente no outro aplicativo,
- Algumas empresas não economizam uma boa parte do seu orçamento que é gasto em softwares de escritório, por conta da falta de conhecimento de um bom software substituto gratuito e para não lidar com o treinamento dos funcionários, ou para não ter que se preocupar em portar os dados para o novo software com todos os impactos já citados anteriormente que esta ação pode acarretar? Converter os formatos dos arquivos é demorado? Para o caso de um sistema web, eles têm uma API com suporte para terceiros?

Consideremos o caso hipotético de uma pequena empresa que utiliza um sistema com cadastro de clientes, e faz esses cadastros há anos pagando reajustes de mensalidades do software cada vez mais caros, seria viável transferir para outro

software? Mesmo que seja mais barato, qual é o ônus de ter que cadastrar todos os clientes novamente no outro software? Nessa situação hipotética podemos imaginar o mau que o aprisionamento tecnológico pode vir a causar.

A adaptação com a nova solução pode vir junto com uma série de trabalhos e se esses custos forem elevados desestimulam a decisão pela mudança de tal forma que a organização se vê presa a aquele produto de TI. Se a solução de TI em que a organização está aprisionada por algum motivo é descontinuada, sofre um encarecimento ou até mesmo se ela muda seus termos de uso, isso pode acarretar grandes prejuízos para a organização aprisionada.

Shapiro e Varian (2003) em sua obra apresentam uma lista de tipos de aprisionamento que podem ocorrer com seus custos de troca associados que aqui reproduzimos na Tabela 1.

Tabela 1. Tipos de Aprimoramento e Custos de Troca a Eles Associados.

Tipo de aprisionamento	Custo de troca
Compromissos contratuais	Indenização compensatórias ou liquidadas
Compras de bens duráveis	Substituição de equipamentos; tende a cair à medida que o bem durável envelhece.
Treinamento em marca específica	Aprender sobre um novo sistema, tanto custo direto quanto perda de produtividade; tende a aumentar com o tempo
Informação de bando de dados	Conversão de dados para novo formato; tende a aumentar ao longo do tempo à medida que a coleção aumenta
Fornecedores especializados	Financiamento de novo fornecedor; pode aumentar com o tempo se as aptidões forem de encontrar/manter
Custos de busca	Custo combinados do comprador e do fornecedor; incluem o aprendizado sobre a qualidade de alternativas
Programas de lealdade	Quaisquer benefícios perdidos do fornecedor titular, mais a possível necessidade de reconstruir o uso cumulativo

Como se pode perceber dos tipos apresentados na tabela acima, o aprisionamento pode se dar das mais diversas formas, desde dificuldades de mudança por compromissos contratuais a questões de aprendizado.

Podemos entender então, que o impacto do aprisionamento pode se apresentar não só sob o aspecto técnico, mas também sobre diversas outras formas tais como obstáculo à evolução tecnológica, impactos na produtividade, maior esforço e custo financeiro para a mudança dentre outros.

E ainda como Shapiro e Varian (1999) lembram:

> "...o aprisionamento é uma moeda de duas faces; você pode detectá-lo como consumidor ou abraçá-lo como fornecedor. De qualquer forma, você tem de compreender os custos de troca e estar apto a antecipá-los e medi-los."

Um dos aspectos tratados por Shapiro e Varian (1999) em sua abordagem sobre o tema do aprisionamento é a relevante questão de uma solução a ser adotada poder ser "aberta" ou "fechada". Um ponto interessante levantado pelos autores é a de decisão envolvendo este tema quando se analisa sob o seguinte prisma: apesar de uma solução aberta em um primeiro momento parecer extremamente atrativa e mais convidativa, um fornecedor de software pode ter uma solução não proprietária e aberta, de funcionalidade limitada, em contrapartida a solução de um outro fornecedor com uma solução proprietária, mas com um desempenho muito melhor.

Esta questão gera o impasse de decisão de, estando com olho nos custos de troca e antecipação de eventuais problemas futuros, inclusive de produtividade e efetividade, qual delas deveria ser escolhida. Por esta situação já se percebe que a fuga da situação de aprisionamento não é uma coisa simples e trivial de decisão fácil, ela pode trazer com ela uma série de pontos que tornam a tarefa de decidir por solução que aprisione e solução que não aprisione uma tarefa bem mais complexa e que, portanto, precisa ser bem analisada e planejada com a definição de uma abordagem estratégica de longo prazo.

Na visão destes autores, a identificação antecipada da situação de aprisionamento, ajuda na proteção de seus efeitos adversos e até cria a possibilidade de usá-lo em seu proveito quando possível. Refletem ainda que em muitos mercados que envolvem o armazenamento, a manipulação ou a transmissão de informação, o aprisionamento nuclear, tangível, é substancial, e é possível fazer ou perder fortunas ao se antecipar ou negligenciar esse papel. Assim defendem que a forma de vencer nos mercados com custos de troca não é evitar o aprisionamento nem adotá-lo. Você precisa pensar de maneira estratégica: olhar para o futuro e pensar no passado.

A abordagem de Shapiro e Varian é feita sob a ótica da economia, mas neste trabalho focaremos nos desdobramentos dos efeitos do aprisionamento dentro da área de atuação da tecnologia da informação.

Outro ponto é que apesar de o problema do aprisionamento conforme exposto até aqui poder se apresentar também sob o ponto de vista pessoal, nossa abordagem neste trabalho se dará exclusivamente sob o ponto de vista organizacional.

2.2 Padrões

Baseado na abordagem de Giozza (1986) sobre padronização da forma de comunicação em redes locais, podemos entender que o padrão tecnológico tem não só por finalidade facilitar a interconexão de soluções heterogêneas, mas também viabilizar a geração em maior escala de soluções de forma a tornar mais acessível (seja tanto a nível de disponibilidade quanto de custo) e o uso mais generalizado da solução. Estes padrões passam então a ser uma importante referência no projeto e na disponibilização de novas soluções de tecnologia. Mas ele alerta que a existência prematura de um padrão pode se constituir em um freio ao invés de estímulo ao uso e o desenvolvimento de soluções.

Em seu livro Redes de Computadores, Tanembaum (1994) em sua abordagem sobre a padronização de redes apresenta um histórico sobre os primórdios das redes de computadores onde cada fabricante de computadores tinha seus próprios protocolos de comunicação. Só a IBM, diz ele, tinha mais de uma dúzia. Como resultado os usuários que tinham computadores de vários fabricantes não conseguiam conectá-los em uma única rede. Esta situação, a que ele denomina de caos, acabou levando muitos usuários a demandar uma padronização. Na sequência ele tece abordagem similar ao de Giozza (1986) em relação às vantagens como produção em massa e a economia de escala advindas da padronização.

Se um “padrão” (na verdade uma solução proprietária), é definido por uma única pessoa ou por uma única empresa, isto pode representar um risco para os consumidores de produtos que trabalhem com esta solução. Uma empresa pode definir este “padrão” de maneira que seja favorável às suas implementações e desfavorável às implementações alheias. Esta prática desfavorece a competição honesta e facilita a criação de monopólios (CERQUEIRA, 2017, p. 2),

Ainda em relação a padrões, Tanembaum (1994) apresenta uma definição em duas categorias: os padrões *de facto* (“de fato”, em latim) e padrões *de jure* (“de direito”, em latim).

O padrão *de facto* são aqueles que se estabelecem sem um processo de geração de padrão formal, é uma adoção de tecnologia já existente como, por exemplo, soluções proprietárias que posteriormente vieram a se tornar um padrão de facto da indústria tais como a Ethernet e o próprio conjunto de protocolos TCP/IP.

O padrão *de jure* são os padrões formais, legais, emitidos por entidades de padronizações autorizadas como a ISO (International Standards Organization), e as americanas IEEE (Institute of Eletrical and Electronicas Engineers), ANSI (American National Standards Institute), etc. Estas entidades acabam sendo divididas em duas classes: aquelas estabelecidas através de acordos entre governos e as organizações voluntárias, fora de acordos.

Um exemplo de organização voluntária é a ISO fundada em 1946 e que possui entre seus membros inúmeras organizações nacionais de padronização como é o caso da ABNT (Associação Brasileira de Normas Técnicas) e da ANSI americana.

Uma forma de trabalho adotado pela ISO para geração de padrões de forma que se alcance o maior consenso possível, é a formação de um grupo de trabalho para produzir uma proposta de representação (Draft Proposal – DP) que é enviada a todos os órgão membros que tem um prazo para criticá-la. Se aprovada pela maioria um documento revisado denominado Padrão Internacional de Representação (Draft International Standard – DIS) é gerado e distribuído para comentários e votação. Com base nos resultados obtidos desta fase o texto final do padrão internacional (International Standard – IS) é aprovado e publicado. Todo este processo começa efetivamente quando qualquer dos membros percebe a necessidade de um padrão internacional em alguma área de atuação.

Assim como o alerta de Giozza, Tanembaum destaca que se o padrão é escrito cedo demais o assunto pode não estar completamente entendido e gerar maus padrões e se forem escritos tarde demais as empresas já poderão ter feito investimentos em fazer as coisas de forma diferente (soluções proprietárias) fazendo então com que estes padrões de jure sejam simplesmente ignorados.

Um padrão recém emitido de grande importância para o momento atual das soluções de tecnologia, e para o tema deste trabalho, colocado a disposição do mercado é o padrão ISO/IEC 19941:2017 - Computação em nuvem — Interoperabilidade e portabilidade que tem por objetivo garantir que todas as partes envolvidas na computação em nuvem, particularmente CSCs (Cloud Service Customer - Cliente de Serviço em Nuvem), CSPs (Cloud Service Provider - Provedor de Serviços em Nuvem) e parceiros de serviços em nuvem (CSNs - Cloud Service Partner) que atuam como desenvolvedores de serviços em nuvem, tenham um entendimento comum de interoperabilidade e portabilidade para suas necessidades específicas. Esse entendimento comum ajuda a obter interoperabilidade e portabilidade na computação em nuvem, estabelecendo terminologia e conceitos comuns (ISO/IEC 19941:2017).

Como o próprio documento afirma, ele é de particular interesse dos stakeholders (partes interessadas) em nuvem com foco em contratos de serviços em nuvem relativos à interoperabilidade ou portabilidade entre serviços em nuvem (ISO/IEC 19941:2017).

Outro ponto de análise, é que em geral, os produtos de software seguem alguma especificação, que determina como eles estruturam as informações com que trabalham e como disponibilizam essas informações para manipulação e visualização (CERQUEIRA, 2017, p. 1).

Uma especificação pode também ser considerada um padrão, quando há um acordo entre várias partes sobre como deve ser essa especificação. Isso significa que a especificação em questão deve passar por um processo de adoção em massa. Esse processo pode acontecer por vários motivos: por obrigação legal, por ser a especificação de um produto que é dominante em seu segmento ou talvez até mesmo por acaso (CERQUEIRA, 2017, p. 1-2).

Segundo os autores, outro tipo de organização que define padrões são consórcios de empresas e indivíduos, que por meio do consenso constroem os seus padrões.

Um exemplo destas organizações é a *World Wide Web Consortium* (W3C), responsável pela definição de padrões para a *Web*, como *HTML*, *CSS* e *XML*.

A *Web* só se tornou viável porque os padrões definidos pela *W3C* são padrões abertos. Não há impedimentos técnicos ou legais para a criação de páginas

Web ou navegadores *Web*, no que diz respeito à utilização destes padrões. A *W3C* tem forte atuação no Brasil e trabalha na definição de padrões para a infraestrutura brasileira. A *W3C* Brasil criou o decálogo da *Web* brasileira, que determina algumas diretrizes para nortear a nossa infraestrutura. Dentre elas, está a organização em padrões, que devem ser abertos e interoperáveis. Esta diretriz é a base para várias outras (CERQUEIRA, 2017, p. 3).

Podemos citar outro consórcio que define padrões com base no consenso é a Organization for the Advancement of Structured Information Standards - OASIS. Dentre vários outros padrões, esta organização é responsável também pelo OpenDocument Format (ODF), usado para documentos de texto (odt), planilhas (ods), apresentações (odp) e diagramas (odg) (CERQUEIRA, 2017, p. 3). Os padrões criados para softwares de escritório, extensões de documentos de edição de texto ODF (Open Document Format) e de planilhas eletrônicas (ODS), junto com softwares livres para a edição dos mesmo como o LibreOffice, ajudaram na descentralização e independência computacional ou até operacional de softwares proprietários que geram uma grande dependência, monopólio e aprisionamento tecnológico nas corporações, com o Microsoft Office.

Como exemplo mais recente de esforço de se encontrar um caminho comum temos a iniciativa consorciada com a participação de várias gigantes da tecnologia como Apple, Facebook, Google, Microsoft e Twitter que criaram em 2018 o Data Transfer Project (Projeto de Transferência de Dados) que é uma ação para criar uma solução de uma plataforma de código aberto que faça a portabilidade de dados serviço-a-serviço no qual qualquer indivíduo presente na web possa facilmente mover seus dados entre provedores de serviço online sempre que quiserem (Data Transfer Project, 2018).

Outro exemplo que poderíamos considerar é a tecnologia bluetooth hoje amplamente utilizada em diversos tipos de dispositivos de uma série de fabricantes. Esta tecnologia começou a ser desenvolvida em 1994 pela Ericsson que pesquisava uma tecnologia capaz de permitir a comunicação entre telefones celulares e acessórios utilizando sinais de rádio de baixo custo em vez dos tradicionais cabos. Posteriormente este projeto despertou o interesse de outras empresas criando-se então o consórcio Bluetooth SIG (Bluetooth Special Interest Group), formado pelas

companhias Ericsson, Intel, IBM, Toshiba e Nokia e dezenas de outras companhias que foram aderindo ao consórcio com o passar do tempo.

2.2.1 Padrões abertos x código aberto

Segundo Cerqueira (2017) é comum a confusão entre os termos "padrão aberto" e "código aberto", entretanto eles não significam a mesma coisa. O padrão aberto é uma especificação a ser seguida e que está disponível para quem desejar implementar uma solução a partir dela. O código aberto é uma das implementações desse padrão, que promove a possibilidade de livre consulta, examinação ou modificação do produto, sem a necessidade de pagar uma licença comercial. A implementação de um padrão aberto não tem que obrigatoriamente ser de código aberto.

Um exemplo que ilustra melhor essa diferença é a relação entre a linguagem de marcação *HTML* e os navegadores *Web*. O HTML é um padrão aberto, mantido pela *W3C*. Porém os navegadores *Web* são os responsáveis por ler documentos *HTML* e apresentar as informações desse documento ao usuário (CERQUEIRA, 2017, p. 3).

> Existem inúmeros navegadores Web, alguns são de código aberto, como o Firefox e o *Chromium*, outros são de código fechado, como o *Edge*, o *Safari* e o *Chrome*. Entretanto, o que todos esses navegadores têm em comum é que eles aderem ao padrão HTML, o que permite que o usuário possa escolher qual navegador utilizar, sem medo de que as páginas Web não sejam apresentadas corretamente (CERQUEIRA, 2017, p. 3).

Outro exemplo é a linguagem *SQL*, um padrão mantido pela ISO. Existem diversos sistemas gerenciadores de bancos de dados relacionais, como *MySQL*, *PostgreSQL*, *Oracle* e *DB2*. Os dois primeiros são de código aberto, e os outros dois são de código fechado. Porém, em todos eles é possível usar a linguagem SQL para criar e manipular os dados (CERQUEIRA, 2017, p. 3).

2.2.2 Portabilidade e interoperabilidade

De acordo com os termos definidos na norma ISO/IEC 17788:2014, a portabilidade de aplicativos é descrita como a "habilidade de migrar um aplicativo de

um serviço para outro serviço" enquanto a portabilidade de dados é descrita como "Portabilidade de dados de um serviço para outro serviço".

De forma complementar podemos definir portabilidade conforme abaixo:

> Portability is a characteristic attributed to a computer program if it can be used in an operating system other than the one in which it was created without requiring major rework. Porting is the task of doing any work necessary to make the computer program run in the new environment. Portability has usually meant some work when moving an application program to another operating system. (TEACHTARGET, 2022)

Desde antes da grande popularização da informática com o advento dos PCs (Personal Computer) a portabilidade sempre foi um desafio para a área de tecnologia e continua sendo. O movimento de downsizing (migrar do mainframe para o ambiente cliente/servidor) há décadas atrás exigiu grandes ações das empresas de portar sistemas e base de dados antes hospedados em grandes mainframes para outras plataformas em ambientes Unix ou Windows Server com arquiteturas e organizações totalmente diferentes. Muitos destes sistemas tiveram que ser reescritos quase que na íntegra. Acompanhando esta popularização dos PCs como já abordado anteriormente ocorreu o advento das redes locais de computadores (LAN) com várias tecnologias concorrentes no mercado e incompatíveis entre si como Ethernet, Token Ring etc.

Diante desta babel e dos altos custos decorrentes, a postura do mercado acabou por exigir das fabricantes soluções compatíveis entre si que não obrigassem a completa troca de todo o aparato tecnológico para continuar viabilizando o crescimento do uso destes recursos nas empresas em prol do negócio.

A portabilidade nasce do contexto de que nada adianta conceder vários direitos aos indivíduos sem dotá-los de ferramentas efetivas para que esses busquem serviços que respeitem os seus direitos ou que tenham políticas que mais lhe agradem.

Desta forma, se visa incentivar e estimular a migração e o livre trânsito de consumidores, sejam eles pessoas ou empresas, entre os diferentes serviços ou produtos do mercado digital.

O projeto citado anteriormente neste trabalho, o DTP (Data Transfer Poject) foi desenvolvido para testar conceitos e viabilidade de transferência de tipos específicos de dados do usuário entre serviços online. Sua finalidade é permitir uma

conexão entre quaisquer duas interfaces de produto voltadas para o público para importação e exportação de dados diretamente. Ele é uma iniciativa de código aberto que procura melhorar o ecossistema de portabilidade de dados, reduzindo a carga de infraestrutura para provedores e usuários procurando também aumentar o número de serviços que oferecem portabilidade (DATA TRANSFER PROJECT, 2018).

A exigência de portabilidade pode ser acompanhada de uma outra exigência denominada interoperabilidade, que pode ser definida conforme abaixo:

> Interoperability refers to the basic ability of computerized systems to connect and communicate with one another readily, even if they were developed by widely different manufacturers in different industries. Being able to exchange information between applications, databases, and other computer systems is crucial for the modern economy. (O'CONNOR, 2017)

A interoperabilidade é descrita na Global Information Infrastructure terminology (ITU-T Y.101) como: "A habilidade de dois ou mais sistemas ou aplicativos em trocar informações e utilizar a informação trocada mutuamente". A ISO/IEC 19941:2017 que trata da interoperabilidade e portabilidade em computação em nuvem, além das definições básicas para as palavras:

- “**Interoperability** - ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged
- **Data portability** - ability to easily transfer data from one system to another without being required to re-enter data.”
- trás diversos outros termos derivados de interoperabilidade e portabilidade tais como (ISO/IEC 19941:2017):
- “**Cloud interoperability** - ability of a CSC’s system to interact with a cloud service or the ability for one cloud service to interact with other cloud services by exchanging information according to a prescribed method to obtain predictable results.”
- “**Transport interoperability** - interoperability where information exchange uses an established communication infrastructure between the participating systems.”
- “**Cloud data portability** - data portability (3.2.1) from one cloud service to another cloud service or between a CSC’s system and a cloud service.”

- “**Data semantic portability** - data portability such that the meaning of the data model is understood within the context of a subject area by the target.”

Dentre as considerações que esta norma procura endereçar sobre portabilidade está a questão da limitação de situações de aprisionamento em que o CSC está vinculado aos serviços em nuvem de um CSP. (ISO/IEC 19941:2017)

No decorrer do seu texto a norma diz “Data portability is a key consideration when considering lock-in to a specific cloud service. Although application portability can affect the cost of migrating between systems, application migration is largely a cost issue and although economic lock-in is a real possibility, it can be mitigated.“. (ISO/IEC 19941:2017)

Quanto à interoperabilidade ela aborda que “Connected devices can capture and upload cloud service customer data to various cloud services using applications running on the device. Such cloud services are of ‘application capabilities type’. The cloud service customer data can also be available to other applications on the original connected device. These scenarios represent interoperability between applications and device platforms of the connected devices on one end, and cloud services on the other. Such a degree of interoperability can help prevent platform or provider lock-in.”. (ISO/IEC 19941:2017)

Como podemos perceber pelo abordado até aqui, a existência de padrões, de capacidade de prover portabilidade e de interoperabilidade, não só para os serviços de computação em nuvem, mas para todas as demais soluções de TI, são fortes mecanismos que podem ajudar a evitar, ou ao menos mitigar, os riscos associados a situações de aprisionamento tecnológico.

2.3 Governança

Segundo Barros (2016) as abordagens envolvendo o conceito da Governança Corporativa se iniciou na década de 1930, com o desenvolvimento dos mercados de capitais, principal mecanismo de financiamento e fomento ao crescimento das empresas. Ainda que o termo não fosse utilizado até o final dos anos 70, suas questões centrais já tinham sido abordadas por Berle e Means em 1932, quando

propuseram o problema da Teoria da Agência, que trata dos conflitos de interesses entre acionistas, gestores, credores e funcionários de uma empresa.

Em 2001 uma série de escândalos financeiros envolvendo grandes corporações norte-americanas por fraude em relatórios financeiros abalou a confiança dos investidores e governo, trazendo à tona a discussão sobre responsabilidade fiscal e governança corporativa. (BARROS, 2016, p. 18)

Segundo Hélder Castro a governança corporativa (GC) surgiu a partir de uma ação reflexiva em torno da ética, a qual versa sobre a discussão acerca das relações entre o mundo corporativo e a sociedade, entre as empresas de uma mesma cadeia de negócios e, dentro das companhias, entre os acionistas, os conselhos e a direção executiva.

O principal objetivo da governança corporativa é garantir a confiabilidade das empresas por meio de um conjunto de mecanismos de acompanhamento que assegurem a conduta correta dos executivos, prezando pelos princípios de transparência (*disclosure*), equidade (*fairness*), prestação de contas (*accountability*) e o respeito ao cumprimento das leis (*compliance*).

Visando manter a transparência e confiabilidade da gestão dos recursos a governança vem se desenvolvendo, pois muitas vezes o gestor não é o dono da organização ou, ele mantém sociedade com acionistas que querem segurança no seu investimento.

Analisando a formação da palavra governança percebemos que é o uso da palavra governar, que segundo o dicionário Houaiss significa:

- Ter mando, direção; dirigir, administrar
- Controlar, dirigir ou fortemente influenciar as ações e o comportamento de (algo ou alguém)

Com o sufixo ‘ança’, que dá a palavra o significado de “Estado” ou “Ação ou resultado dela” (LACOTIZ, 2006).

Assim, a governança pode ser entendida como um conjunto de processos, costumes, políticas, leis, regulamentos e instruções que regulam a maneira como uma empresa é dirigida, administrada ou controlada.

2.3.1 Governança de tecnologia da informação

A Governança de TI (GTI) se relaciona diretamente com a Governança Corporativa (GC), motivo pelo qual se tornou um assunto predominante na alta gestão das empresas, através de processos que trazem estas garantias e permitem que as organizações atinjam seus objetivos.

Diversos modelos foram desenvolvidos e constantemente passam por revisões para apoiar os executivos na melhoria de processos, na mensuração de valores, de ativos tangíveis e intangíveis da organização (BARROS, 2016, p. 10).

> Para toda infraestrutura, recursos e informações necessárias para a utilização da TI existem no mercado modelos de gestão de TI e governança de TI que controlam, sustentam administrativa e tecnicamente a TI. Contudo, a definição dos termos não estão ainda bem empregadas no meio acadêmico, divergindo tanto em sua definição quanto em sua aplicação (MOREIRA, 2014, p. 2)

Segundo definição emitida no COBIT 4.1 (2007) a governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização. Assim a governança de TI se refere à estrutura e processos associados a TI que as organizações usam para tentar garantir que suas operações de TI apoiem as metas e objetivos globais da organização.

De acordo com o Instituto de Governança de TI, os objetivos de governança aplicáveis a praticamente qualquer organização incluem alinhar a estratégia de TI com a estratégia da empresa, alocando os recursos de TI de forma eficiente para apoiar a realização dos objetivos organizacionais e agregar o valor previsto pelos investimentos em TI e gerenciar de forma eficaz os riscos relacionados com TI.

Seguindo estudos de Fernandes e Abreu (2014) às integrações tecnológicas de processos através da tecnologia da informação (aplicações e infraestrutura computacional e de comunicação de dados) fazem com que o risco que a TI (Tecnologia da Informação) representa para a continuidade do negócio seja altamente visível. É óbvio que tal risco deve ser mitigado e contingenciado de uma forma sem precedentes e não imaginada até então.

Com base no abordado até aqui, podemos observar que o risco de aprisionamento tecnológico pode representar um grande risco para toda a organização caso não seja devidamente identificado, dimensionado e tratado. Aqui

cabe relembrar a afirmação de Shapiro e Varian (1999) que apresentamos anteriormente neste trabalho de que, para uma empresa diminuir seu aprisionamento a uma solução ela precisa ser capaz de visualizar os desdobramentos futuros para poder traçar uma estratégia que reduza a dependência de determinada solução.

Vale ressaltar que grande parte das melhores práticas aplicáveis à TI já está disponível há vários anos e somente a partir de 2005 os administradores “acordaram” para a necessidade da boa gestão das atividades de TI. Até o mais desavisado dos administradores (aquele que não entende a TI da sua empresa) já percebeu o risco que é para o seu negócio uma TI mal gerenciada, pois provavelmente já precisou lidar com um incidente de indisponibilidade ou perda de dados de aplicações críticas (FERNANDES; ABREU, 2014, p. 9).

Para diversas organizações, a informação e a tecnologia que a suporta é seu ativo mais valioso, mas muitas vezes é o menos compreendido. Organizações de sucesso reconhecem os benefícios da tecnologia da informação e a utilizam para transmitir os valores das partes interessadas do negócio.

Entender e gerenciar os riscos associados é de grande importância, existem dependência crítica de muitos processos de negócios em relação a TI. Há uma inevitabilidade de avaliar o valor da TI, o gerenciamento de riscos de TI e a crescente necessidade de controle sobre as informações são agora entendidos como elementos-chave da governança corporativa. Valor, risco e controle são a essência da governança de TI.

Denota-se, que as organizações devem atender aos requisitos de qualidade, retenção e segurança para suas informações e todos os seus ativos. Os executivos também devem otimizar o uso dos recursos de TI disponíveis, incluindo aplicativos, informações, infraestrutura e pessoas. Os executivos precisam entender o estado atual de sua TI e decidir quais controles implementar, para isso é necessário saber da meta básica da política, implementar planos e procedimentos, bem como a estrutura organizacional designada para prover razoável garantia de que os objetivos de negócio serão atingidos e de que eventos indesejáveis serão prevenidos ou detectados e corrigidos.

O gerenciamento do risco (proposto pelas boas práticas de governança), permite que a organização reconheça todos os riscos (e oportunidades) derivados

da TI para o negócio e que decida e tenha planos para mitigá-los na medida que julgue necessário. O Gerenciamento dos Recursos de TI assegura a gestão dos recursos mais importantes para TI: recursos humanos e recursos tecnológicos (informações, infraestrutura, aplicações). Promove a valorização do conhecimento e da infraestrutura (BARROS, 2016, p. 19).

Fica claro que o gerenciamento de risco deve ser desdobrado em outras medidas que permitam a organização se cercarem de um conjunto de ações derivados de processos e controles que efetivamente atuem sobre a necessidade de organização e a forma de execução das atividades de TI e os recursos que ela venha a incorporar.

Basicamente o que toda boa prática de governança propõe é um conjunto de medidas estruturadas voltadas para planejar, construir, executar e monitorar de forma que as ações de TI retornem o melhor resultado para suas organizações.

A implantação de processos e controles como o de planejamento envolvendo atividades de TI que permitam antever situações que englobam todos os recursos de TI (sejam eles infraestrutura, aplicativos e pessoas) e de forma que a área de TI esteja habilitada a entregar as informações que a organização precisa para seus negócios, busca dentre outras coisas gerenciar os riscos e garantir a segurança destes recursos de TI dos quais a organização é tão dependente.

As ações de governança devem procurar garantir que a geração e o tratamento da informação que a organização necessita observe os seguintes critérios:

- Efetividade – que a informação seja relevante e pertinente para o processo de negócio assim como seja entregue em tempo, de maneira correta, consistente e utilizável.
- Eficiência – a informação tem que ser entregue através do melhor (mais produtivo e econômico) uso dos recursos.
- Integridade - informação fidedigna e completa bem como observe adequação aos valores de negócios.
- Disponibilidade – a informação poder ser gerada, tratada e acessada, sempre que necessária pelo processo de negócio hoje e no futuro.

Em sua avaliação e tratamento dos riscos, a organização através de processos bem desenhados, deve procurar garantir que nenhum risco, incluso o de aprisionamento, causará ou viabilizará a violação de qualquer um destes critérios.

Assim, além da identificação e gerenciamento de riscos, processos como a definição de qual direcionamento tecnológico a organização adotará, como ela identifica as soluções que aporta no seu ambiente, como ela faz este aporte e mantém os softwares aplicativos e infraestrutura em seu ambiente, além da forma como instala e homologa as soluções e assegura a continuidade dos serviços, estão intimamente ligados a tarefa de se evitar ou ao menos mitigar o risco de aprisionamento tecnológico.

Há inúmeros modelos disponíveis no mercado que podem auxiliar nesta tarefa. Na figura abaixo, destacamos alguns deles.

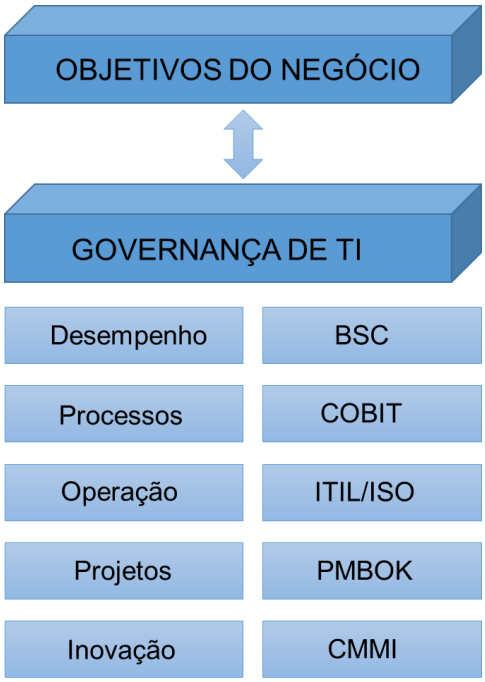

Figura 2. Principais modelos
Fonte: Adaptado de COBIT

Segundo Barros (2016) boas práticas como o COBIT, fornecem um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI. Ele ajuda as organizações a criar valor por meio da TI mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos.

Um outro modelo disponível que podemos citar é a norma ABNT ISO/IEC 38500:2018 - Governança de TI para a Organização que também aborda a Governança de TI e tem descrito como seu objetivo promover o uso eficaz, eficiente e aceitável de TI. Dentre os princípios que ela estabelece estão os de:

- Estratégia, que é o princípio que se refere também a necessidade de que os planos para uso da TI atendam às necessidades atuais e contínuas da organização e,
- Aquisição, sob o qual as aquisições devem ser baseadas em análises apropriadas com tomadas de decisões claras equilibrando adequadamente os benefícios as oportunidades, os custos e os riscos tanto a curto quanto a longo prazo.

Seu modelo define também três tarefas principais:

- Avaliar o uso atual e futuro da TI
- Dirigir, preparar e implementar estratégias e políticas que garantam que o uso da TI atenda aos objetivos de negócio e,
- Monitoração do desempenho em relação as estratégias

O que se pode depreender destes modelos é que na etapa de planejar do processo de governança, devem ser consideradas questões como, se ao longo do tempo os recursos de TI (aplicativos, infraestrutura e pessoas) são aportados adequadamente, se são apropriados e se seu uso estão otimizados, se os riscos estão sendo identificados e gerenciados e se a qualidade destes recursos é adequada às necessidades de informação da organização. Na etapa do construir a preocupação é se estes recursos, incluindo as novas soluções, vão atender as necessidades do negócio, sendo aportadas tempestivamente e dentro do padrão necessário, se funcionarão e se integrarão adequadamente conforme necessidade da organização e quais alterações que podem ocorrer sem afetar as operações de negócio.

Como destacam Shapiro e Varian (1999) em sua obra, no tratamento de eventuais situações de aprisionamento é necessário pensar de maneira estratégica, olhando o futuro, mas pensando no passado, assim a incorporação desta nova preocupação nas práticas que provêm a governança de TI na organização já é um ótimo instrumento para tentar evitá-lo ou ao menos mitigá-lo.

Segundo a ABNT em sua norma 38500:2018, a boa governança de TI ajuda as organizações a garantirem que o uso da TI (inclusive em seu uso atual e futuro) contribua positivamente para o seu melhor desempenho dentre outras razões por implementação e operação apropriadas de ativos de TI, a clareza da responsabilidade e responsabilização pelo fornecimento e demanda de TI na consecução dos objetivos da organização, na continuidade do negócio, pela alocação eficiente de recursos, pelas boas práticas nos relacionamentos com as partes interessadas e pela concretização dos benefícios esperados nos investimentos de TI.

Na próxima seção deste trabalho, iremos fazer uma análise sobre como boas práticas de governança podem vir a auxiliar as organizações em relação ao tema do aprisionamento tecnológico.

3. APRISIONAMENTO TECNOLÓGICO - MEDIDAS DE PREVENÇÃO

Apesar de a análise a seguir ter se baseado em modelos para implementação da governança de TI como o COBIT e a ISO nas organizações, ela não tem a pretensão de defender um modelo ou outro nem tratar de forma detalhada pela ótica do modelo o problema do aprisionamento tecnológico. Dessa forma, na abordagem a seguir não haverá referência direta a processos de qualquer modelo. A proposta aqui é discutir como a ideia geral de uma boa prática recomendada quando aplicada, pode auxiliar a organização no objetivo de se evitar ou mitigar o risco de aprisionamento tecnológico.

Como pudemos observar nas seções anteriores a preocupação com a situação de risco é uma abordagem comum a todos os modelos de boas práticas de governança.

Pudemos entender também ao longo do trabalho que a instalação de uma situação de aprisionamento tecnológico na organização é um risco bastante presente, agravada pelo volume e celeridade com que novas soluções de TI são criadas e pela dinâmica do negócio que exige que elas sejam incorporadas de forma rápida para atender e proporcionar melhorias no tratamento das informações para auxiliar no alcance dos objetivos de negócio.

Soluções de TI como os de mensageria eletrônica WhatsApp e Telegram que surgiram há poucos anos, já foram incorporadas como ferramenta de relação entre empregados para tratar de problemas internos e até como instrumento de negociação de vendas das organizações tendo substituído, mesmo que parcialmente, o uso dos serviços de correio eletrônico.

Outras soluções também recentes como os serviços de computação em nuvem ganham cada vez mais adeptos e vem substituindo os data centers de diversas organizações ao redor do mundo.

Em relação ao aporte de soluções, Shapiro e Varian fazem a seguinte análise: “Suponhamos que você esteja para selecionar uma marca de software para formar um banco de dados fundamental para sua atividade. Uma consideração importante nessa decisão deve ser a da dificuldade de converter seu arquivo de dados para outros formatos daqui a alguns anos. Você deve também estar bem informado para saber se dependerá ou não de um único fornecedor para aperfeiçoar

o banco de dados no futuro. A avaliação adequada desses custos de troca antes que ocorra o aprisionamento pode valer milhões de dólares para sua organização ao longo do caminho.”

E ainda:

“A estratégia básica para compradores de tecnologia de informação que antecipam o aprisionamento consiste em dois elementos fundamentais:

• Negociar com firmeza no início do ciclo de aprisionamento por um “adoçante” ou alguma forma de proteção de longo prazo antes de ficar aprisionado.

• Tomar providências para minimizar seus custos de troca ao longo do ciclo de aprisionamento.”

“Comece a gerir seus custos de troca antes de tê-los. Em outras palavras, desde o início você deve estruturar sua relação para maximizar suas opções adiante no ciclo de aprisionamento.”

“Uma abordagem semelhante consiste em escolher um sistema “aberto” desde o início, de modo que você não fique preso a um único fornecedor.”

Segundo Cerqueira (2017) a melhor maneira de evitar os problemas decorrentes do *aprisionamento tecnológico* é buscar tecnologias e serviços que prezam pela *interoperabilidade e pela portabilidade.* Em grande parte, o que torna isso possível são os padrões abertos e a descentralização, mas também é possível que a organização otimize situações como esta através da observância de boas práticas recomendadas por frameworks de governança de TI.

Partindo deste ponto, vamos analisar a seguir como algumas destas boas práticas podem vir a auxiliar a organização no tratamento do aprisionamento tecnológico.

Uma das boas práticas recomendada por frameworks de governança, propõe que a organização implemente processo que viabilize a determinação de qual o direcionamento tecnológico que ela adotará quando de seus aportes de tecnologia. Esta prática procura fazer com que as organizações consigam analisar de forma prévia tanto as tecnologias existentes como também as emergentes para que se identifique as mais adequadas a concretização das estratégias de TI. Esta análise deve incluir também as estratégias de migração e aspectos contingenciais dos componentes de infraestrutura. Ela deve levar em consideração a possibilidade

de eventuais mudanças no ambiente de sistemas de informação, e procurar prover melhorias na interoperabilidade entre plataformas e aplicações.

A indicação de que preferencialmente as soluções de TI a serem adotadas sejam aderentes a padrões internacionais estabelecidos e produzidos por organismos reconhecidos auxiliam na tarefa de se evitar o aprisionamento tecnológico.

As tendências futuras das tecnologias já incorporadas e as emergentes passíveis de incorporação devem ser analisadas de forma a se antever situações que possam se caracterizar em risco futuro incluindo o de aprisionamento. Esta boa prática sugere ainda que se avalie a conformidade com padrões já definidos levando em consideração aspectos como relevância para o negócio e os riscos associados.

Como se pode observar, com este controle que esta prática proporcionará a organização poderá procurar analisar de forma antecipada todos os aspectos de uma determinada solução em termos de aderência a padrões já definidos, e a capacidade de interoperabilidade e portabilidade de forma a evitar que futuramente ela esteja aprisionada a uma solução específica que foi, ou se pretende que seja adotada, ou então que, no mínimo, estejam mitigados os impactos negativos de um eventual aprisionamento. É fato que existem uma série de outros aspectos técnicos e financeiros relevantes que devem ser também analisados com a adoção desta prática de governança, mas deve-se garantir que a questão de aprisionamento tecnológico seja um destes.

Em um artigo disponível em Teleco (2022)*, um site especializado em temas da área de telecomunicações, há uma interessante abordagem sobre como decidir sobre a incorporação de uma nova solução observando-se critérios que acabam por permitir a proteção ao aprisionamento dos quais destacamos alguns que de forma adaptada podem ser aplicáveis a TI:

“Num mundo globalizado e em convergência, a escolha de um padrão tecnológico, é vital. Muitos fatores devem ser considerados, como os aspectos técnicos; serviços a serem providos; considerações de ordem política; aspectos econômicos, produtivos e comerciais; riscos envolvidos; universalização; impacto social e outros. O importante é que a decisão tenha por base um balanço dessas considerações.

Entretanto, há certos pontos-chaves que não se podem ignorar (TELECO, 2022), eles são;

- Flexibilidade do Sistema: diz respeito à versatilidade de uso universal. O uso de plataformas abertas universais e não proprietárias previsão de aplicações futuras. Afinal a tecnologia precisa ser adaptada durante a evolução do negócio e deve durar tempo suficiente para remunerar os investimentos;
- Interoperabilidade: os sistemas têm que ser interoperáveis para permitir interconexões e formação de redes complexas compostas de vários sistemas diferentes;
- Maturidade: maturidade de sistema ou equipamentos significa: produtos e tecnologias testadas no mercado e debugadas nos últimos 5 anos; amplo número de aplicações disponíveis e em enorme crescimento; todas debugadas, ou seja, eliminação dos riscos inerentes a novos projetos;
- Escala Econômica e Industrial: significa benefícios econômicos; receptores mais baratos e disponíveis para o consumidor, implementação bem sucedida, tecnologia madura e provada, menores riscos e enormes mercados mundiais; enormes oportunidades de fabricação e de comércio, baixo custos industriais e disponibilidade de tecnologia e de insumos;

Como se pode observar, se estas diretrizes e orientações já tem por base a observância de aspectos de padrões de indústria recomendados por organismos internacionais, ou de acordo entre diversos fabricantes, interoperabilidade e portabilidade, na incorporação de novas soluções de tecnologia na organização, se antecipa e se desvia de situações de eventual aprisionamento futuro.

O COBIT versão 4.1 e versão 5 definem risco respetivamente como:

“Risco (Risk) – Em negócios, o potencial de que uma certa ameaça irá explorar as vulnerabilidades de um recurso ou grupo de recursos para causar perda e/ou prejuízos; usualmente medido por uma combinação de impacto e probabilidade de ocorrência” (COBIT 4.1, 2007).

“A combinação da probabilidade de um evento e suas consequências (ISO/IEC 73)” (COBIT 5, 2012).

Já a ABNT em sua norma 38500:2018 define (com destaque nosso para as duas notas que acompanham a definição):

“Risco – efeito da incerteza nos objetivos. Nota 1: um efeito é um desvio em relação ao esperado – positivo e/ou negativo. Nota 2: Os efeitos negativos refletem ameaças, enquanto riscos positivos refletem oportunidades.”

No caso de aprisionamento tecnológico este risco (com efeitos negativos) se caracteriza pela potencial ameaça de a solução de TI já implantada ou a ser implantada venha a prejudicar o negócio quando for necessária a sua integração e/ou interação com outras soluções de TI já implantadas ou a serem implantadas, não proporcionando então a devida interoperabilidade e a portabilidade, bem como vir a apresentar um custo bastante onerado para sua troca ou modificação em razão de fatores financeiros, operacionais ou técnicos e podendo ainda se desdobrar, em razão desta não interação, integração, modificação ou troca, em prejuízos operacionais ou financeiros ao negócio.

Assim a possibilidade de sua ocorrência futura na incorporação de uma nova solução de TI, ou mesmo sua já presença deve ser avaliado e gerenciado. Ao avaliar e gerenciar os riscos de TI, esta preocupação deve ser feita uma considerada pela estrutura de gestão de riscos de TI para que seja alinhada com a de gestão de riscos da organização.

A incorporação desta nova preocupação na boa prática de governança de avaliação e gerenciamento de risco já existente ou a ser implantada permitirá que, quando da avaliação de uma nova solução de TI, sejam feitas ações de identificação e dimensionamento da ameaça real de a organização se colocar em situação de aprisionamento tecnológico e qual o potencial impacto negativo nos objetivos ou nas operações da organização permitindo decidir então com base nisto, se o risco é aceitável ou não.

Avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos ajuda a identificar um possível e já existente aprisionamento tecnológico tanto de software como em hardware. A probabilidade e o impacto associado ao risco devem ser determinados individualmente.

Caso o aprisionamento já esteja presente, ou mesmo se decida por incorporá-lo seja por qual justificativa for, deve-se desenvolver e manter um processo de respostas a este risco para assegurar que controles com uma

adequada relação custo-benefício mitiguem a demasiada exposição ao risco que está ou estará presente.

Assim, o processo de resposta ao risco deve identificar estratégias de como evitar, reduzir, compartilhar ou mesmo aceitar o risco de aprisionamento tecnológico, considerando os níveis de tolerância aceitáveis. Uma vez aceito ou identificado existente, o risco ele deve passar a fazer parte do plano de ação de risco com monitoramento frequente.

Outra boa prática é a de que sempre que houver a necessidade de incorporação de uma nova tecnologia requer seja feita uma análise prévia à aquisição ou ao desenvolvimento para assegurar que ela seja eficaz e eficiente inclusive a longo prazo. Este processo deve contemplar a definição das necessidades, considerar fontes alternativas, a revisão de considerar a viabilidade econômica e tecnológica, mas deve-se considerar também as a execução das análises de risco e de custo-benefício incluindo a de risco de aprisionamento tecnológico para a obtenção de uma decisão final.

Nesta avaliação deve-se não só identificar e especificar os requisitos técnicos e funcionais que o negócio necessita e que a solução provê, mas também identificar, documentar e analisar os riscos associados, incluso o de aprisionamento tecnológico, que a solução possa estar trazendo para a organização. A partir desta análise deve-se verificar a viabilidade e conveniência da aceitação do risco em caso de confirmação de presença de possibilidade de aprisionamento futuro.

Na execução desta prática, as análises devem se atentar aos padrões emitidos por entidades de padronizações autorizadas aos quais a solução se adequa e a existência de alguma solução de código aberto dentre as alternativas avaliadas, como uma forma de escapar de eventuais prejuízos que podem ser causados pelo aprisionamento tecnológico.

A utilização de softwares de código aberto ou código proprietário devem ser consideradas de acordo com as reais necessidades da empresa, medindo vantagens e desvantagens, e caso se decida por solução de código proprietário, estar atento se esse software oferece compatibilidade com padrões abertos para poder realizar futuras migrações ou até exportações de outras fontes de dados.

A decisão final quanto à escolha da solução deve ser tomada pelo patrocinador do negócio, mas com a apresentação e a devida orientação técnica sobre todos os seus prós e contras feitos pela área de TI.

Uma outra boa prática de governança que também auxilia neste processo de se procurar evitar ou mitigar o aprisionamento tecnológico é o da aquisição e manutenção de aplicativos e de infraestrutura. Esta prática está associada a preparação efetiva visando o aporte de soluções de TI na organização.

Esta prática deve procurar incluir controles e requisitos de segurança apropriados, a análise do hardware/software e a sua configuração de acordo com padrões estabelecidos que possam dar certo grau de garantia quanto à prevenção de aprisionamento tecnológico. Esta aquisição deve levar em consideração o direcionamento tecnológico adotado na organização e os requisitos de segurança, disponibilidade, interoperabilidade e portabilidade em resposta aos riscos identificados e em linha com a arquitetura de segurança da informação e o perfil de tolerância a riscos da organização.

Outro ponto que deve ser considerado são as condições envolvendo eventuais atualizações na infraestrutura de tecnologia que poderiam ser demandadas no futuro. Para tanto deve se ter uma abordagem planejada não só para a aquisição, mas também para manutenção e proteção da infraestrutura em alinhamento com as políticas de direcionamento tecnológico definidos.

Assim é importante a elaboração de um plano que defina a aquisição, a implementação e a manutenção da infraestrutura tecnológica de forma que não só atenda aos requisitos técnicos e funcionais estabelecidos pelo negócio, mas que estejam também de acordo com a direção tecnológica adotada pela organização contemplando em seu teor as questões relacionadas ao aprisionamento tecnológico.

Quando o aprisionamento for inevitável procurar desenvolver uma estratégia e um plano para manutenção da infraestrutura que procure reduzir os impactos deste aprisionamento para os negócios ao mesmo tempo em que se procure assegurar rotas seguras para se tentar sair desta situação assim que possível.

Outra boa prática, relacionada agora a efetiva aquisição de uma solução de TI requer a definição e a aplicação de procedimentos claros de aquisição, e em especial a de seleção de fornecedores. Necessário se ter atenção especial no estabelecimento das regras contratuais e de aquisição propriamente ditas que

procurem já em seus termos reduzir os impactos de aprisionamento. Assim assegura-se que a organização tenha todos os recursos de TI sempre que necessário e mantendo a relação custo-benefício.

Atenção especial deve ser dada a procedimentos para modificar e rescindir contratos com fornecedores de soluções que causam aprisionamento tecnológico. O procedimento deve contemplar no mínimo as formalidades legais, financeiras, organizacionais, documentais, de desempenho, de disponibilidade das informações tratadas, de segurança e as responsabilidades e obrigações legais em casos de cancelamento, incluindo cláusulas de penalidades. Deve-se procurar garantir que os interesses da organização sejam protegidos em todos os contratos de aquisição e ao mesmo tempo se certificar que a forma como o contrato foi estruturado e escrito, não será ele próprio, o motivo do aprisionamento.

A seleção dos fornecedores deve ser feita de acordo com a prática formal e justa que assegure a melhor opção viável com base nos requisitos que foram definidos pela organização e com base em informações dadas pelos fornecedores em potencial e quando possível através de avaliações de outros clientes da solução de TI.

É necessário ter em mente que, como a TI hoje permeia praticamente toda a organização, a qualquer risco a que a TI se expõe, na prática expõe todo o negócio podendo prejudicá-lo de maneira bastante acentuada.

Na nossa abordagem foram tratadas de forma genérica, sem entrar em maiores detalhamentos, apenas algumas práticas de boa governança recomendadas por modelos mundialmente aceitos, que consideramos essenciais por estarem associadas a questões de visão estratégica, para auxiliar a organização a tratar melhor a questão do aprisionamento tecnológico em seu ambiente computacional.

É necessário que se entenda que pode haver inúmeras outras práticas também recomendadas que podem auxiliar a organização nesta tarefa de prevenção e tratamento de aprisionamento tecnológico e não só as elencadas aqui neste trabalho. Práticas que procurem assegurar a continuidade dos serviços, o desempenho e a capacidade, o gerenciamento da configuração e o gerenciamento de serviços de fornecedores dentre outras, podem também ser de grande ajuda nesta tarefa. Por isto é muito importante que se entenda de forma plena o conceito e

as situações de geração de aprisionamento e que se esteja atento a toda e qualquer ação que possa auxiliar nesta tarefa de mitigação ou eliminação.

Já havendo a adoção de práticas de governança de TI na organização a preocupação passa a ser a de colocar no radar o risco, a prevenção e o tratamento de situações de aprisionamento tecnológico. Em não havendo ainda a adoção de práticas de governança, é importante que o corpo diretivo entenda os ganhos possíveis com sua adoção e de que as mesmas devem não só endereçar as questões relacionadas a aprisionamento, mas também a uma série de outras relevantes para a organização que com certeza trarão grandes benefícios para o negócio.

Dentre as três lições básicas para compradores de soluções de TI apresentadas por Shapiro e Varian (2003), podemos destacar duas em especial nas quais as práticas de governança são de grande valia:

“Temos três lições básicas para os compradores de sistemas de informação e tecnologia:

- Siga estratégias como a da segunda fonte de fornecimento e a de sistemas abertos para minimizar a amplitude de seu aprisionamento. Mesmo que você tenha de fazer investimentos em uma determinada tecnologia, você pode ainda planejar à frente para evitar tornar-se preso a um único fornecedor.
- Olhe adiante para a próxima vez que escolher um fornecedor e tome providências logo de início para aumentar seu poder de barganha quando essa ocasião chegar. Tenha informações sobre seu relacionamento com o fornecedor, como registros de manutenção, e use padrões que possam reduzir os custos se você tiver de trocar de fornecedor. Esses serão ativos valiosos se você decidir romper seu relacionamento”

Como se pode perceber, a efetiva ação de dirigir, gerenciar e controlar é a que permite efetivamente criar capacidade de ver antecipadamente possíveis situações futuras, identificar obstáculos e definir caminhos de forma a se ter um melhor, mais seguro e mais otimizado trajeto para que o negócio da organização consiga alcançar seus objetivos sem maiores sobressaltos.

4. CONCLUSÃO

A importância da informação para as organizações é universalmente aceita, constituindo, senão o mais importante, pelo menos um dos recursos cuja gestão e aproveitamento estão diretamente relacionados com o sucesso desejado.

A informação também é considerada e utilizada em muitas organizações como um fator de estrutura e um instrumento de gestão. Portanto, a gestão efetiva de uma organização requer a percepção objetiva e precisa dos valores da informação e do sistema de informação.

O trabalho da governança em TI para colaborar com a alinhamento estratégico da organização vai além da eficiência e produtividade, ele também conta com a gestão de riscos ao longo do tempo. O aprisionamento tecnológico sendo um dos grandes riscos da TI deve ser levado em consideração e recomenda-se que medidas sejam tomadas para minimizá-lo, às vezes até em detrimento de produtividade a vantagem financeira a curto prazo.

O aprisionamento tecnológico é um grave problema que abrange tecnologias dos mais diversos segmentos. No segmento da informação, porém, ele é especialmente crítico, já que a perda de informação pode ser um desastre para muitas organizações, inclusive porque com as novas legislações e leia da informação as empresas precisam manter uma certa historicidade dos dados, a perda de informações pode representar além de desvantagem estratégia um empecilho jurídico.

Para evitar o aprisionamento da organização em uma tecnologia que não faz mais sentido, seja economicamente ou estrategicamente, é recomendado adotar práticas recomendadas pela governança de TI.

O uso de tecnologias que não trabalhem ou não ofereçam suporte adequado a padrões abertos e que privilegiam padrões fechados oferecem risco de aprisionamento da informação e devem ser bem estudadas e com contratos bem planejados caso sejam a solução escolhida.

Como pode ser observado durante nossa abordagem as organizações podem ter muitos ganhos ao incorporar em suas práticas a preocupação com o aprisionamento tecnológico. A adoção de alguns procedimentos citados permitirá a mesma ter maior controle sobre seu ambiente computacional identificando como se

encontra e quais caminhos decidirá trilhar para sair ou se manter fora de situações de aprisionamento.

Vivemos em uma era que há a cada dia um grande volume de novas soluções tecnológicas sendo apresentadas ao mercado. Se olharmos nas duas últimas décadas para cá veremos o enorme salto tecnológico pelo qual o mundo passou, transformando a vida e o modo de fazer as coisas das pessoas e das empresas. O simples olhar dessa forma, o aprender com o passado como dizem Shapiro e Varian, já dá a noção do grau de preocupação que se deve dar ao assunto do aprisionamento.

Como trabalhos futuros podemos identificar a necessidade de uma pesquisa de campo de forma a se mapear a real situação de empresas brasileiras frente ao assunto, se elas têm real noção de sua existência e até de presença em seu ambiente computacional bem como as práticas que a mesma adotam para combatê-lo.

REFERÊNCIAS BIBLIOGRÁFICAS

ALECRIM, Emerson. Bluetooth: o que é, como funciona e versões. **Infowester**, 2021. Disponível em: https://www.infowester.com/bluetooth.php#historia. Acesso em: 10 de dezembro de 2021.

ANASTÁCIO, Wellington Montefusco. **Fatores críticos de sucesso para integração com sistemas legados: um estudo de caso no SERPRO**. 2014. Tese de Doutorado. Universidade de São Paulo.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO/IEC 38500:2018 – Governança da TI para a organização, 2018.

BARROS, Conrado Gomes de Queiroz. Governança de TI: estudo das boas práticas sobre alinhamento das estratégias de TI e negócio. 2016. Disponível em: https://app.uff.br/riuff/handle/1/7407. Acesso em: 09 de março de 2022.

CASTRO, Hélder. Como surgiu a Governança Corporativa? Uma breve discussão contextual. **Administradores**, 2014. Disponível em: https://administradores.com.br/artigos/como-surgiu-a-governanca-corporativa-uma-breve-discussao-contextual. Acesso em 10 de dezembro de 2021.

CERQUEIRA, Hugo. Aprisionamento Tecnológico. **WritewhitConfidence**, 2017.

CHIAVENATO, I. **Introdução À Teoria Geral Da Administração**. 9 ed. São Paulo: Manole, 2014 p. 296,418

CHIMENDES, Vanessa Cristhina Gatto; NEVES,José Manoel Souza das. **A Implantação de Tecnologia da Informação Contribuindo Para a Melhoria do Processo de Gestão na Área de Logística**. Niterói – RJ: VI Congresso Nacional de Excelência em Gestão, 2010. Disponível em: https://www.inovarse.org/sites/default/files/T10_0325_1146_3.pdf. Acesso em: 09 de março de 2022.

COBIT 2019 Foundation, Governance Institute.

COBIT 4.1 - Modelo, Objetivos de Controle, Diretrizes de Gerenciamento, Modelos de Maturidade. 2007. IT Governance Institute

COBIT 5 - Habilitando Processos. 2012. ISACA

Data Transfer Project Overview and Fundamentals. 2018. DTP

DE CARVALHO, Jeferson et al. Comunicação e Consumo na Web: do ambiente participativo à tentativa de aprisionamento tecnológico. **Revista Eletrônica do Programa de Pós-graduação da Faculdade Cásper Líbero**. V. 4, Ano 4, 2012. Disponível em: https://www.researchgate.net/profile/Rafael-Vergili/publication/250309506_Comunicacao_e_Consumo_na_Web_do_ambiente_participativo_a_tentativa_de_aprisionamento_tecnologico/links/00b4951eac935a5772000000/Comunicacao-e-Consumo-na-Web-do-ambiente-participativo-a-tentativa-de-aprisionamento-tecnologico.pdf. Acesso em: 09 de março de 2022.

ENGELBERT, Ricardo; GRAEML, Alexandre. Custos de Troca em Tecnologia da Informação: a Proposição de um Modelo Taxonômico Integrado a partir da Literatura. **Revista Organizações em Contexto**, v. 7, n. 13, p. 157-184. Disponível

em: https://doi.org/10.15603/1982-8756/roc.v7n13p157-184. Acesso em: 09 de março de 2022.

FERNANDES, Aguinaldo Aragon; DE ABREU, Vladimir Ferraz. **Implantando a Governança de TI-: Da estratégia à Gestão de Processos e Serviços**. Brasport, 2014.

GIOZZA, William Ferreira et al. **Redes Locais de Computadores - Tecnologia e Aplicações**. Editora McGraw-Hill, 1986.

HERNÁNDEZ SAMPIERI, Roberto; FERNÁNDEZ COLLADO, Carlos; BAPTISTA LUCIO, María del Pilar. Metodologia de pesquisa. **Porto Alegre: Penso**, 2013.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **COBIT® 2019 Framework: Governance and Management Objectives**. ISACA, 2018.

International Organization for Standardization. ISO/IEC 19941:2017: Information technology — Cloud computing — Interoperability and portability, 2017 Disponível em: https://www.iso.org/standard/66639.html. Acesso em: 09 de março de 2022.

LACOTIZ, Andréa. A Análise dos Sufixos–ança/-ença,-ância/-ência na obra do simbolista João da Cruz e Souza. **Estudos Linguísticos XXXV. São Paulo: USP**, 2006. Disponível em: http://www.usp.br/gmhp/publ/LacA1.pdf. Acesso em: 10 de dezembro de 2021.

MACIEL, Edemir Reginaldo. **Aprisionamento na infraestrutura de tecnologia da informação.** Dra. Leticia Mara Peres. Pag. 101. Dissertação (Mestrado) – Informática, Ciências Exatas, Universidade Federal do Paraná, Curitiba, 2018. Disponível em: https://hdl.handle.net/1884/58419. Acesso em: 09 de março de 2022.

MACIEL, Edemir Reginaldo. Aprisionamento na infraestrutura de tecnologia de informação, 2018.

MOREIRA, Allan Winckler; NETO, Julio Vieira. Diferenças entre gestão de TI e governança de TI–uma breve comparação. In: **Congresso Nacional de Excelência em Gestão, n. X**. 2014. p. 11. Disponível em: https://www.inovarse.org/sites/default/files/T14_0075.pdf. Acesso em: 09 de março de 2022.

NFUKA, Edephonce N.; RUSU, Lazar. **Critical success factors for effective it governance in the public sector organisations in a developing country: the case of tanzania.** 18th European Conference on Information Systems. 2010. Disponível em: https://aisel.aisnet.org/ecis2010/128/. Acesso em: 09/03/2022

O'CONNOR, Stephen. **What Is Interoperability, and Why Is it Important?** ADVANCED DATA SYSTEMS CORPORATION, 2017. Disponível em: https://www.adsc.com/blog/what-is-interoperability-and-why-is-it-important#:~:text=Interoperability%20refers%20to%20the%20basic,different%20manufacturers%20in%20different%20industries. Acesso em: 09 de março de 2022.

SHAPIRO, Carl e VARIAN, Hal R. **A economia da informação: como os princípios econômicos se aplicam à era da Internet.** 14ª impressão. Elsevier, 1999.

TANENBAUM, Andrew Stuart. Redes de Computadores, 1994.

TEACHTARGET. **What is portability? - Definition from WhatIs.com**. 2022. Disponível em: https://www.techtarget.com/searchstorage/definition/portability. Acesso em: 10 de março de 2022.

TELECO. **Seção: Tutoriais Operação – Padrões Tecnológicos**. 2022. Disponível em: https://www.teleco.com.br/tutoriais/tutorialrisco/pagina_4.asp. Acesso em: 10 de março de 2022.

WEILL, P.; ROSS, J. **IT governance**: how top performers manage IT decisions rights for superior results. Watertown: Harvard Business School Press, 2006.

WU, T. **The Master Switch**: The Rise and Fall of Information Empires. New York: Alfred A. Knopf, 2010.