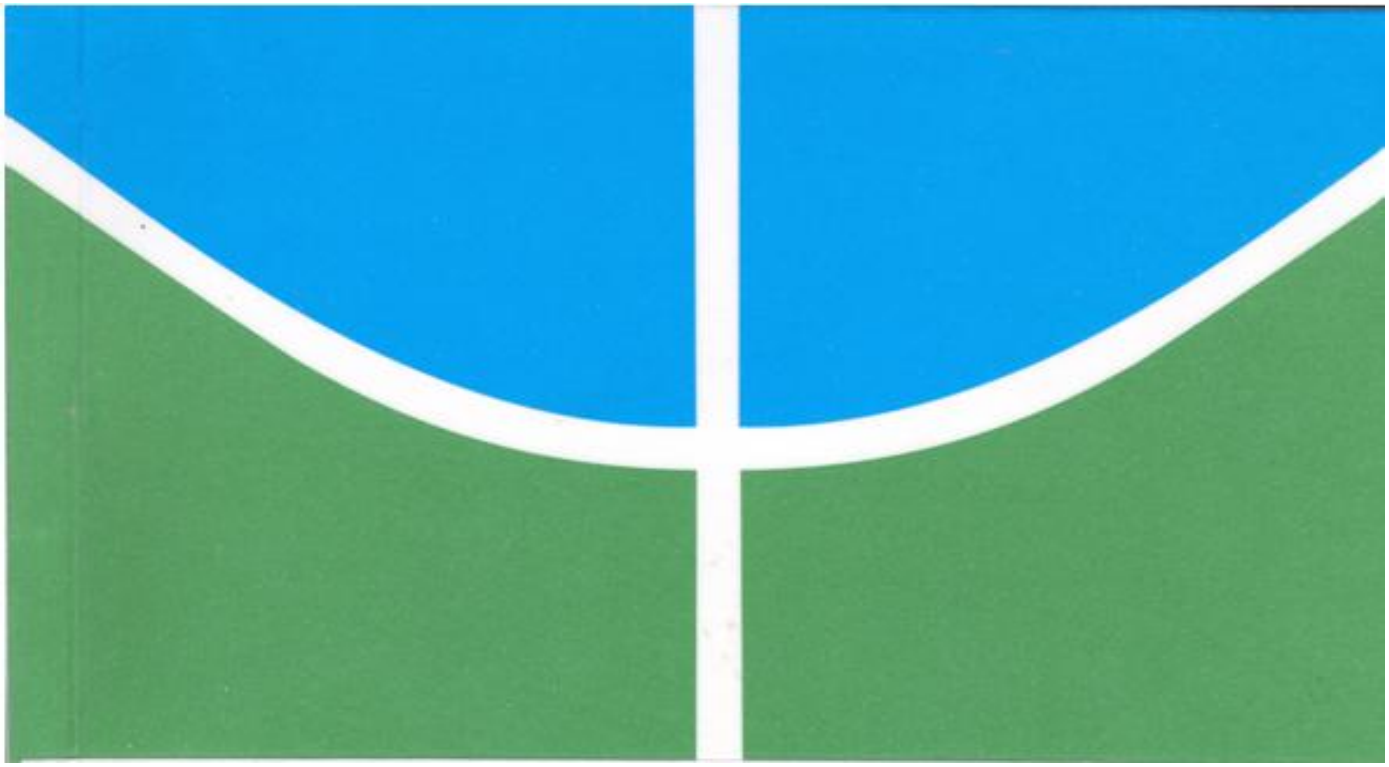


INTEGRAÇÃO DA SEGURANÇA NA GESTÃO DE TI: UMA PROPOSTA DE ABORDAGEM SISTÊMICA

ELIANE CARNEIRO SOARES

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

INTEGRAÇÃO DA SEGURANÇA NA GESTÃO DE TI: UMA PROPOSTA DE ABORDAGEM SISTÊMICA

ELIANE CARNEIRO SOARES

ORIENTADOR: LUIS FERNANDO RAMOS MOLINARO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.DM - 446/2011
BRASÍLIA / DF: JULHO/2011

Ficha catalográfica elaborada pela Biblioteca Central da Universidade de Brasília. Acervo 991624.

Soares, Eliane Carneiro.
S676i Integração da segurança na gestão de TI : uma proposta de abordagem sistêmica / Eliane Carneiro Soares. -- 2011.
xvi, 100 f. : il. ; 30 cm.

Dissertação (mestrado) - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, 2011.
Inclui bibliografia.
Orientação: Luis Fernando Ramos Molinaro.

1. Tecnologia da informação. 2. Sistemas de segurança. 3. Governança corporativa. I. Molinaro, Luis Fernando Ramos. II. Título.

CDU 658:004

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

INTEGRAÇÃO DA SEGURANÇA NA GESTÃO DE TI: UMA PROPOSTA DE ABORDAGEM SISTÊMICA

ELIANE CARNEIRO SOARES

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

LUIS FERNANDO RAMOS MOLINARO, Doutor, ENE/UnB
(ORIENTADOR)

JOÃO MELLO, Doutor, UNB
(EXAMINADOR INTERNO)

DANIELA FÁVARO GARROSSINI, Doutora, UNB
(EXAMINADOR INTERNO)

BRASÍLIA/DF, 28 DE JULHO DE 2011.

REFERÊNCIA BIBLIOGRÁFICA

SOARES, Eliane Carneiro (2011). Integração da Segurança na Gestão de TI: uma proposta de abordagem sistêmica Dissertação de Mestrado em Engenharia Elétrica, Publicação ENE.DM – 446, 28/Jul/2011, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 100p.

CESSÃO DE DIREITOS

AUTOR: Eliane Carneiro Soares.
TÍTULO: Integração da Segurança na Gestão de TI: uma proposta de abordagem sistêmica.
GRAU: Mestre ANO: 2011

ELIANE CARNEIRO SOARES
2ª AVENIDA BLOCO 1060 CASA 02, NÚCLEO BANDEIRANTE
CEP 71.715-028 – Brasília – DF – Brasil

“Que Deus nos dê a sabedoria dos simples e a humildade dos mestres
para que possamos continuar nossos estudos
em busca do conhecimento fraterno e
divisível entre todos.”

Geanete Lavorato

Ao meu filho Eduardo, por quem tudo vale à pena.

E, aos meus Pais: Airton e Angélica, pelo exemplo de luta e determinação.

AGRADECIMENTOS

Primeiramente a Deus pelo dom da vida e pela imensurável força concedida para lutar pelos sonhos e ter perseverança no desejo de continuar crescendo intelectual e profissionalmente.

Ao meu filho, Eduardo. Ele é o principal responsável por minha dedicação e empenho. Por suportar ausência nesses dias e pelo imenso amor e carinho que tornou possível realizar este sonho.

Aos meus pais, Airton e Angélica, pelo exemplo de determinação fundamental para a realização deste sonho. Às minhas irmãs, Márcia e Andréa, pelo companheirismo. Aos meus sobrinhos, Mickael, Guilherme, Júlia e Isadora, pelo tempo subtraído do convívio, e ao meu cunhado Carlos James, pela amizade, admiração e respeito, com palavras certas na hora certa.

Ao grande amigo Laerte Peotta, por ter compartilhado este sonho comigo desde a primeira linha.

Ao corpo docente da Universidade de Brasília, em especial ao meu orientador, Professor Luís Fernando Ramos Molinaro, pela orientação, amizade e, principalmente, pela oportunidade de crescimento intelectual e profissional.

A toda equipe de trabalho do Núcleo de Multimídia e Internet, em especial à Daniela Garrossini, Ana Carolina Kalume, Guilherme Pereira Souto e Marcelo Fernandes, pelo incentivo constante.

Aos amigos queridos: Rita de Cássia Amorim, Amanda Albuquerque, Aparecida Pinheiro, Sílvia Taraleskof, Cleonice D'Ábadia, Susi Martinelli, Ana Paula e Rogério Carrijo, Priscila Suzano, Evandro Lorens, Rafael Farnese e Luis Carlos de Castro, que sempre me apoiaram e contribuíram direta ou indiretamente na realização deste trabalho, e por todo apoio e paciência, principalmente nesses meses de intensa dedicação.

À Secretaria de Estado de Educação do Distrito Federal, por investir nos seus servidores e acreditar no aperfeiçoamento profissional como forma de melhorar a qualidade do ensino.

RESUMO

INTEGRAÇÃO DA SEGURANÇA NA GESTÃO DE TI: UMA PROPOSTA DE ABORDAGEM SISTÊMICA

Autor: Eliane Carneiro Soares

Orientador: Dr. Luís Fernando Ramos Molinaro

Programa de Pós-Graduação em Tecnologia

Brasília, 28 de julho de 2011.

A presente dissertação tem como objetivo realizar uma pesquisa, por meio de um estudo de caso, que integre a Segurança à gestão de Tecnologia da Informação (TI) e apóie o processo de governança e gestão das organizações. A proposta centra-se na obtenção do alinhamento entre o negócio e a TI por meio da utilização do modelo de arquitetura corporativa, descrito pelos subsistemas, Direcionamento, Desenvolvimento e Entrega, incorporados à concepção sistêmica de organização (Funcionalidade, Processos e Estrutura), como forma de buscar informações sobre os processos internos de uma organização rumo ao entendimento organizacional com foco na melhoria contínua dos processos e da estrutura. Durante o trabalho será empreendido um estudo de caso sobre o uso das normas que referenciam a segurança da informação, em especial as ISO/IEC 27001 e ISO/IEC 27002, e as utilize como eixo norteador para a aplicação dos controles necessários intrínsecos à organização.

Palavras chaves: Segurança da Informação, Gestão e Governança de TI

ABSTRACT

SECURITY MANAGEMENT IT INTEGRATION: PROPOSAL FOR A SYSTEMIC APPROACH

Author: Eliane Carneiro Soares

Supervisor: Dr. Luís Fernando Ramos Molinaro

Programa de Pós-Graduação em Tecnologia

Brasília, 28 of July of 2011

This paper aims to conduct an investigation through a case study, which integrates the management of the Security of Information Technology (IT) and supports the process of governance and management of organizations. The proposal focuses on achieving alignment between business and IT through the use of the architecture model, described subsystems by Direction, Development and Delivery, incorporated into the design of systemic organization (functionality, processes and structure) as a way to seek information about the internal processes of an organization into the organizational understanding with a focus on continuous improvement of processes and structure. The work will undertake a case study on the use of rules that refer to information security, in particular the ISO / IEC 27001 and ISO / IEC 27002, and the use of guidelines for implementing the necessary intrinsic controls for the organization.

Key Words: Security Information, IT Management and Governance

SUMÁRIO

LISTA FIGURAS

LISTA TABELAS

LISTA DE QUADROS

ACRÔNIMOS E ABREVIAÇÕES

BSC	*Balanced Score Card*
BSI	*British Standart Institute*
CGG	Ciclo de Governança e Gestão
CMMI	*Capability Maturity Management Integration*
COBIT	*Control Objectives for Information and Related Technology*
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
CRM	*Customer Relationship Management*
FCS	Fatores Críticos de Sucesso
GC	Gestão do Conhecimento
IBGC	Instituto Brasileiro de Governança Corporativa
IEC	*International Electrotechnical Commission*
ISACA	*Information Systems Audit and Control Association*
ISACF	*Information Systems Audit and Control Foundation*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infraestructured Library*
ITSM	*IT Service Management*
ITSMF	*Information Technology Service Management Forum*
OGC	*Office of Government Commerce*
PMI	*Project Management Institute*
PDCA	*Plan-Do-Check-Act*
SI	Sistemas de informação
SGSI	Sistema de gestão da segurança da informação
TI	Tecnologia da Informação

1 INTRODUÇÃO

A contemporaneidade é caracterizada por grandes transformações do ponto de vista da globalização e dos crescentes avanços tecnológicos. Nessas duas áreas, a governança e a gestão assumiram papel estratégico nas organizações e tornaram-se fundamentais na geração de valor e qualidade aos negócios. O cenário atual exige das empresas maior consistência com relação ao fluxo informacional interno e externo, além de maior flexibilidade e velocidade nos ajustes necessários à condução das estratégias organizacionais.

Em corporações onde as ligações entre os setores se compõem essencialmente pela comunicação em rede, a revolução tecnológica, por meio da queda de fronteiras regionais, alcançou resultados relevantes em um mundo globalizado. Sem o desenvolvimento da Tecnologia da Informação (TI), seria praticamente impossível viabilizar o aumento, a velocidade e o caráter estratégico do fluxo comunicacional dentro do ambiente organizacional. Os assuntos relacionados à área de TI, em especial a segurança de TI, é um ponto crucial na gestão das organizações devido à importância das redes de comunicação e das informações integradas no apoio ao alcance de objetivos estratégicos para as corporações. O argumento predominante até alguns anos atrás, de que as áreas de uma organização atuam de forma isolada e independente uma das outras, não reflete a necessidade atual das organizações.

> "A integração de processos colaborativos dentro das organizações permite sincronizar elementos, sem entraves burocráticos e repetições de tarefas. Daí porque os dispositivos informacionais se tornaram insubstituíveis para ajustar as empresas às condições mutáveis dos mercados globalizados. A informação é pedra de toque na constituição de dividendos competitivos, credenciando-se como recurso básico de gestão e insumo estratégico para a produção de bens materiais e imateriais". [**1**]

No mercado atual, no cenário das organizações, há uma série de guias ou *frameworks* e normas, como COBIT, ITIL, COSO, CMMI e família ISO/IEC 27000, estão voltados à gestão de TI. Alinhados com os objetivos estratégicos da organização, esses procedimentos atuam diretamente no controle de processos operacionais e auxiliam o desenvolvimento da governança e da gestão organizacional. É por meio do processo de governança que a melhoria continua dos processos existentes em uma organização pode ser

empreendida. Este trabalho está focado na realização de uma análise com vistas ao estabelecimento de uma relação transformacional na modelagem organizacional. Nesse contexto, o processo de mudança necessariamente deve estar pautado na transcrição da realidade e suas ações devem ser descritas em uma relação representada através da cadeia de governança, onde é possível estabelecer um processo de gestão eficiente.

Enquanto a governança corporativa busca criar e descrever um processo de tomada de decisão, a governança corporativa de TI busca um paralelo entre o ambiente tecnológico e o corporativo, buscando subsidiar a área corporativa com informações para uma decisão mais acertada e rápida [**2**]. Assim, a governança corporativa estabelece a estrutura por meio da qual os objetivos da empresa são estabelecidos, define os meios para atingi-los e monitora seu desempenho por meio da qual a governança corporativa incorpora a governança corporativa de TI [**3**].

A governança corporativa de TI, por meio de sua arquitetura, sugere que o alinhamento organizacional deve envolver desde a missão até as infraestruturas tecnológicas que servem de suporte ao negócio da organização. Essa capacidade de representação da arquitetura corporativa permite o refinamento contínuo das tecnologias da informação, sem comprometer o alinhamento com o negócio da organização, favorecendo a permanente retenção de conhecimento para facilitar o processo de tomada de decisão [**4**].

Para complementar a governança de TI, como forma de suprir diversas outras exigências, surge a governança em segurança. Enquanto a TI busca subsidiar informações e disponibilizar sistemas, a governança em segurança busca a qualidade na segurança em relação a essa informação, sua disponibilidade, integridade, confidencialidade e outros fatores considerados importantes a fim de resguardar não só a informação, mas também a imagem da corporação e os itens que a compõem [**2**].

A Segurança da Informação de um negócio é uma necessidade emergente e de ampla aplicação dentro da organização, com escopo de atuação abrangendo todas as áreas. A segurança das informação protege as informações contra uma ampla gama de ameaças e assegura a continuidade dos negócios, minimizando prejuízos e maximinizando o retorno de investimentos e de oportunidades comerciais. Assim, a gestão da segurança trata de um conjunto de regras e práticas que regulam como uma organização gerencia, cria, usa e distribui suas informações de forma segura [**3**].

Nesse contexto, a presente dissertação tem como objetivo realizar uma pesquisa, por meio de um estudo de caso, que busque integrar conceitos relativos à segurança da informação e gestão de TI, como forma de análise dos subsistemas de TI, que incluem Direcionamento, Desenvolvimento e Entrega, na transformação da realidade organizacional. Para isso, serão aplicados conceitos de governança e gestão corporativa de TI no contexto da segurança, bem como o modelo de arquitetura organizacional de TI (Direcionamento, Desenvolvimento e Entrega), de forma a buscar informações dos processos internos de uma organização rumo ao entendimento organizacional e com foco na melhoria contínua dos processos e da estrutura. Durante o trabalho será empreendido um estudo de caso sobre o uso das normas que referenciam a segurança da informação, em especial as ISO/IEC 27001 e ISO/IEC 27002, e as utilize como eixo norteador para a aplicação dos controles necessários intrínsecos à organização.

De forma conjunta, serão aplicados conceitos relativos ao ciclo de governança e gestão alinhado ao PDCA[1], acerca dos domínios de TI: Negócio, Aplicação e Infraestrutura. E, a partir dessa leitura, será empreendida uma análise sistêmica dos seguintes conceitos: *i)* Funcionalidade; *ii)* Processo e, *iii)* Estrutura, como premissa à realização de um resgate sobre a importância da segurança da informação nas organizações, bem como o estabelecimento de um processo de gestão da Segurança da Informação.

A perspectiva traçada no presente trabalho busca não apenas contribuir com a qualidade da gestão da segurança de TI nas organizações, através do conhecimento colaborativo obtido pela integração de modelos e a utilização de normas, bem como propor uma leitura da organização através de seus processos organizacionais responsáveis pela implementação e melhoria contínua da governança corporativa de TI.

[1] O modelo PDCA foi desenvolvido na década de 1930, com base no planejar (*Plan*), executar (*Do*), controlar (*Check*) e agir (*Act*), formam um ciclo de controle estatístico de processos que sugerem melhoria contínua. O PDCA é aplicado para se atingir resultados dentro de um sistema de gestão e pode ser utilizado em qualquer empresa de forma a garantir o sucesso nos negócios, independentemente da área de atuação da empresa.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Realizar uma pesquisa, por meio de um estudo de caso, que integre a Segurança na gestão de Tecnologia da Informação (TI) e apóie o processo de governança e gestão nas organizações, utilizando como controles as normas da família ISO/IEC 27000, a arquitetura corporativa de TI (Direcionamento, Desenvolvimento e Entrega), os domínios Negócio, Aplicação e Infraestrutura e o modelo sistêmico do trio: Funcionalidade, Processo e Estrutura.

1.1.2 Objetivos Específicos

- Observar as funcionalidades da organização como um todo e por partes, similar aos testes de funcionalidade de *software*;
- Observar, analisar e decompor as funcionalidades que pertencem ao Direcionamento, Desenvolvimento e Entrega a fim de caracterizar a atividade destes subsistemas de TI;
- Observar, analisar e decompor as funcionalidades que fazem parte do domínio da organização inseridos no escopo dos subsistemas de TI;
- Observar, analisar e decompor as funcionalidades que pertencem ao modelo sistêmico do trio como forma de caracterizar a atividade destes no escopo do domínio da organização;
- Aplicar os controles necessários, com base nas normas ISO/IEC 27001 e ISO IEC 27002, aos subsistemas de TI preservando sua especificidade e considerando suas funcionalidades descritas no processo de analise descrito anteriormente;
- Aperfeiçoar a governança e a gestão por meio da aplicação dos modelos apresentados.

1.2 ESTRUTURA DO TRABALHO

Esta dissertação está dividida em duas partes, cujos objetivos são o aprofundamento teórico-metodológico e a aplicação de um estudo de caso na organização analisada. O conteúdo proposto centra-se em uma abordagem que integre os conceitos relativos à Segurança aos conceitos de Gestão de Tecnologia da Informação. Na abordagem proposta o modelo de arquitetura corporativa composto pela descrição dos subsistemas de TI, as saber: Direcionamento, Desenvolvimento e Entrega promove um alinhamento entre a TI e o negócio de maneira eficiente e que gere valor à organização. Outros dois modelos também descritos ao longo do trabalho tratam de visões que repartem a organização em: Funcionalidade, Processo e Estrutura e os domínios da organização: Negócio, Aplicação e Infraestrutura.

O primeiro capítulo busca apresentar conceitos básicos da Gestão de Serviços, governança corporativa, ontologia e metamodelagem, governança e gestão de TI descrevendo de maneira objetiva, os históricos, estruturas e principais características.

Faz parte do segundo capítulo, a descrição de uma abordagem realizada à integração da Segurança à Gestão de TI, por meio de uma visão diferenciada de um modelo de gestão. Será demonstrando de que forma as relações existentes e o pontos fortes propiciam a integração dos modelos apresentados.

O terceiro capítulo será um espaço para apresentar a organização estudada, onde será descrito o estudo de caso realizado. Para tal serão apresentadas as etapas do ciclo de governança e gestão de TI com foco na segurança. Esta abordagem refere-se à aplicação transversal da abordagem integradora da segurança à gestão de TI no modelo de arquitetura corporativa composto pelos critérios de Direcionamento, Desenvolvimento e Entrega. Esta abordagem permite a compreensão de conceitos sistêmicos de Funcionalidade, Processos e Estrutura.

O aprofundamento teórico-metodológico integra o quarto capítulo onde serão apresentadas as avaliações e diagnósticos referentes à aplicação da abordagem integradora da segurança à gestão de TI, com relação ao modelo de arquitetura corporativa de TI, composto pelos critérios de Direcionamento, Desenvolvimento e Entrega.

1.3 METODOLOGIA

Para a realização dos objetivos propostos nesta dissertação, a metodologia utilizada foi qualitativa, constituída por duas partes, a saber. Para a primeira parte do trabalho foi utilizada pesquisa descritiva e revisão de literatura, como forma de identificar os melhores conceitos acerca do conteúdo analisado. Na segunda parte foi utilizado o método experimental, por meio de um estudo de caso realizado em um ambiente organizacional.

A pesquisa qualitativa é uma metodologia de pesquisa que pode ser empreendida por meio do método exploratório estruturado como forma de prover percepções e a compreensão do problema. O objetivo fundamental está na interpretação do fenômeno que se observa. Assim, esta interpretação gira em torno da observação, a descrição, a compreensão e o significado. A pesquisa qualitativa considera cada problema objeto de uma pesquisa específica para a qual são necessários instrumentos e procedimentos específicos. Assim, [**5**] descreve cinco atributos referentes à pesquisa qualitativa: *i)* características gerais; *ii)* coleta de dados; *iii)* objeto de estudo; *iv)* interpretação dos resultados e, por fim, *v)* generalização.

O estudo de caso descritivo encontra-se no cerne do entendimento de um fenômeno social complexo [**6**]. Sua aplicação volta-se à descrição de um contexto de vida autêntico no qual o escopo se baseia em uma intervenção ocorrida como forma de estabelecer a lógica de ligação dos dados às proposições do estudo.

Assim, os elementos abordados no estudo de caso foram: *i)* descritivo: descreve o fenômeno dentro de seu contexto; *ii)* planejamento: o desenvolvimento de um estudo de caso único justifica-se pois seu propósito é analisar o ambiente organizacional em que se insere; *iii)* coleta dos dados: os dados coletados são qualitativos onde o recurso para sua obtenção foi a observação; *iv)* análise dos dados: a analise dos dados norteia-se pela descrição do caso, sua adequação ao padrão proposto e a descrição dos controles da família ISO/IEC 27000, reiterados pela validação interna.

De acordo com [**7**] *apud* [**8**] a adoção de métodos qualitativos se justifica sempre que a pesquisa envolver:

- Estudo de sistemas de informação no seu contexto real;
- Estudo de fenômenos complexos, nos quais os fatores contextuais devem ser exaustivamente analisados;
- Descrição e compreensão do estado da arte naquelas situações onde a prática se antecipa à teoria;
- Geração de teorias a partir da prática.

Para o embasamento dessa proposta foi necessário realizar a fundamentação teórica dos documentos ISO/IEC 27001 e ISO/IEC 27002 voltados à Segurança da Informação onde seus controles baseiam-se no modelo *Plan, Check, Do* e *Act* (PDCA). Foi realizada uma pesquisa bibliográfica sobre as teorias de governança e gestão de TI, segurança da informação, que reúne o estudo de vários modelos de arquitetura corporativa.

A utilização do estudo de caso descritivo vem ao encontro do entendimento da integração da segurança na gestão de TI por meio de uma abordagem sistêmica onde, sua aplicação volta-se à descrição de um contexto; especificamente, num laboratório da Universidade de Brasília. Seu escopo se fundamenta na aplicação dentro da organização de modelos de arquitetura corporativa, baseada na interpretação de suas ações por meio de processos e por meio de funcionalidades, inseridas na descrição do modelo de arquitetura corporativa TI representado pelos subsistemas lógicos, denominados Direcionamento, Desenvolvimento e Entrega, que interagem entre si e permitem o alinhamento entre a TI e o negócio, conforme Figura 1.1.

Figura 1.1 – Estrutura de alinhamento entre modelos

A estruturação dos resultados da aplicação do estudo de caso se dará pela descrição da leitura da organização por meio da utilização de tabelas que diferenciem inicialmente os subsistemas de TI e suas especificidades relacionadas. Para cada subsistema de TI realizar-se-á a divisão por etapas do Ciclo de Governança e Gestão (CGG) alinhado aos controles do PDCA. Cada etapa do CGG realizar a abordagem nos domínios: *i*) Negócio, *ii*) Aplicação e *iii*) Infraestrutura e para cada domínio, finalmente, integrará os conceitos sistêmicos: *i*) Funcionalidade, *ii*) Processos e *iii*) Estrutura , conforme representado pela Tabela 1.1.

Tabela 1.1- Estrutura de alinhamento entre modelos

DIRECIONAMENTO		
CGG ALINHADO COM O PDCA	NEGÓCIO	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA
	APLICAÇÃO	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA
	INFRAESTRUTURA	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA
DESENVOLVIMENTO		
CGG ALINHADO COM O PDCA	NEGÓCIO	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA
	APLICAÇÃO	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA
	INFRAESTRUTURA	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA
ENTREGA		
CGG ALINHADO COM O PDCA	NEGÓCIO	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA

	APLICAÇÃO	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA
	INFRAESTRUTURA	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA

2 REFERENCIAL TEÓRICO

2.1 PRINCÍPIOS ONTOLÓGICOS

O termo ontologia vem do grego *ontos*, que significa ser e *logos*, palavra. Embora o estudo do *ser* tenha raízes nos estudos platônicos e aristotélicos, o uso do termo ontologia descreve um ramo da filosofia muito mais recente, com sua introdução na história entre os séculos XVII e XVIII por filósofos alemães [**9**].

Ontologia é a ciência do *ser*, ou o estudo dos seres. Para a Ciência da Computação e a Ciência da Informação, uma ontologia é um modelo de dados que representa um conjunto de conceitos dentro de um domínio e os relacionamentos entre estes. Uma ontologia é utilizada para realizar inferência sobre os objetos do domínio. São utilizadas como uma forma de representação de conhecimento sobre o mundo ou alguma parte deste. Para Gruber, um corpo de conhecimento formalmente representado, sua base deve estar calcada na contextualização de alguns itens, a saber: os objetos, conceitos e outras entidades que existem em alguma área de interesse e as relações que mantêm entre si. A conceituação é uma visão abstrata, simplificada do mundo que desejamos representar para algum propósito. Cada base de conhecimento, ou do agente de nível de conhecimento está comprometida com alguma conceituação, explicita ou implicitamente [**10**].

Uma ontologia é uma especificação explícita de uma conceituação. O termo teve origem na filosofia, onde uma ontologia é um relato sistemático da Existência. Quando o conhecimento de um domínio é representado por meio de um formalismo declarativo, o conjunto de objetos que podem ser representados é chamado de universo do discurso. Este conjunto de objetos, e as relações descritíveis entre eles, refletem-se no vocabulário de representação com a qual um programa de conhecimento representa o conhecimento [**10**].

Percebe-se que o desenvolvimento de uma ontologia para Kühne requer um processo contínuo de interação entre diferentes áreas do conhecimento, mas é possível a distinção de papéis quando o foco sobre a aplicação da ontologia é dada. A ontologia é um modelo de um domínio, reais ou imaginários e o domínio de conceitos na ontologia deve refletir essa realidade que está sendo modelada ou compreendida [**11**].

A proposta de aplicação ontológica cabe em um entendimento do ponto de vista organizacional, que promove a conceituação acerca das funcionalidades, processos e estruturas internas e externas. A ontologia explica o *ser*, dentro da visão organizacional, aplica-se a um contexto referente à um modelo de dados representativo de um conjunto de conceitos e o relacionamento proposto. Explica-se a partir de uma aplicação que irá integrar as áreas organizacionais, por meio de uma visão sistêmica das partes que a constituem.

O presente trabalho utiliza-se da conceituação ontológica como forma de entendimento global do negócio e das partes que o compõem, pois é a partir desta compreensão que se dará o entendimento do todo, sem perder de vista os fatores que levarão à eficácia e eficiência organizacional.

2.1.1 O Processo de Metamodelagem

Metamodelagem define em alto nível métodos e técnicas. Segundo Kühne um modelo é uma abstração de um sistema (real ou baseado em linguagem) permitindo que predições ou inferências sejam feitas. Uma caracterização geral é: um modelo é a descrição de alguma coisa. Um modelo pode ser descrito por três características de acordo com Kühne *apud* Stachowiak: a) Mapeamento: um modelo baseado em seu original, b) Redução: um modelo reflete uma relevante seleção das propriedades do original ou c) Pragmatismo: um modelo necessita ser utilizado no lugar do original a respeito de algum propósito [**11**] [**12**].

Como forma de proporcionar um melhor entendimento acerca da definição de modelo, Kühne remete-o enquanto uma projeção. Assim, as duas primeiras características são de fácil compreensão considerando o pensamento de que um modelo é como uma projeção, que nesta projeção há a implicação que alguma coisa (o original) esboçada e que

uma parcela da informação foi perdida durante o desenho. Desta forma, uma parcela da informação se perde na atividade abstração e a parcela que se reteve irá depender do propósito para o qual o modelo será usado [**11**].

O uso pragmático, por meio de seu efeito prático, de um modelo facilita o entendimento da terceira característica, de acordo com Steinmüller, pois um modelo de informação possui as seguintes descrições: foi desenvolvido por alguém (remetente), sobre alguma coisa (conteúdo), para um destinatário (receptor) e com algum propósito (uso). Desta forma, modelar ou desenhar os processos de negócio de uma organização consiste em identificar, de forma geral, o propósito como um todo, os seus principais processos e os respectivos indicadores de sucesso e em seguida, proporcionar um maior nível de detalhamento por meio de sub-processos, até o nível de atividades normativas ou individuais. [**13**]

O aumento da necessidade e importância da TI com relação ao suporte e viabilização dos processos de negócio faz com que a disponibilidade dos serviços de informação seja crucial para o bom desenvolvimento dos negócios. Não menos importante, percebe-se o envolvimento das questões relacionadas à segurança da informação ao escopo da organização.

De acordo com Weill, na medida em que uma organização caminha rumo ao amadurecimento de sua arquitetura corporativa, esta diminui o percentual de gastos com aplicações locais e infraestrutura. Assim, a partir do contexto deste trabalho pode-se perceber que quanto maior o entendimento acerca dos processos de negócio da organização melhor a qualidade da sua modelagem a respeito do seu funcionamento e, finalmente, um alinhamento efetivo pode ser proporcionado de forma a permitir a observação clara dos pontos que devem ser tratados para atingir as metas desejadas [**14**].

O presente trabalho utiliza-se dos conceitos de processos de modelagem como forma de esboçar os processos de negócio de uma organização, de maneira a aproximar o entendimento com o todo, com os processos e com indicadores de desempenho relacionados.

2.1.2 Modelagem baseada em teste de funcionalidade: o teste da caixa preta e de caixa branca

A modelagem de uma organização confere o nível de aprofundamento suficiente para o atendimento das necessidades que norteiam seu funcionamento, tornando possível a compreensão de que quanto maior o conhecimento a respeito dos processos existentes dentro de uma organização melhor será o desenho de sua arquitetura, detalhada por meio da aplicação da modelagem. Isto com vistas a promoção de forma mais clara e eficiente sobre o alinhamento da organização com suas necessidades.

Modelagem baseada no teste de caixa-branca é uma técnica de teste que usa a perspectiva interna do sistema para modelar os casos de teste. Confrontando com um teste de *software*, a perspectiva interna significa basicamente o código fonte. Comparando com um teste de *hardware*, cada nó de um circuito pode ser testado [**15**].

Ainda tendo como referência testes de funcionalidades de *software*, difere do teste de caixa-preta, onde a perspectiva interna do sistema é desconsiderada, sendo testadas e mensuradas somente as interfaces do sistema. Entretanto, ambas as técnicas podem ser usadas em conjunto, no que é chamado teste de caixa-cinza. Dessa forma, o teste é modelado conhecendo-se a estrutura interna do sistema, mas a execução ignora esse aspecto, como na caixa-preta.

De acordo com Sommerville, o teste de caixa-preta é um teste de *software* para verificar a saída dos dados usando entradas de vários tipos. Tais entradas não são escolhidas conforme a estrutura do programa. Quanto mais entradas são fornecidas, mais rico será o teste. Uma abordagem mais realista para o teste de caixa-preta recai sobre a escolha de um subconjunto de entradas que maximize a riqueza do teste. É possível agrupar subconjuntos de entradas possíveis que são processadas similarmente, de forma a demonstrar que o teste de somente um elemento desse subconjunto serve para averiguar a qualidade de todo o subconjunto [**15**].

A aplicação de técnicas de teste leva o testador a produzir um conjunto de casos de teste (ou situações de teste). Uma abordagem sobre o desenvolvimento do teste de caixa-preta é o teste baseado na especificação, de forma a demonstrar que as funcionalidades são aplicadas de acordo com os requisitos. Apesar de necessário, esse tipo

de teste é insuficiente para identificar certos riscos em um projeto de *software*. O testador não está interessado em como as entradas são processadas, o testador apenas acompanha as saídas produzidas pelo sistema. Ou seja, só são observadas se as saídas são coerentes com as entradas oferecidas.

Estabelecendo uma correlação do teste de caixa branca e do teste de caixa preta sob a ótica da visão sistêmica Jensen *apud* Dietz prega um importante pressuposto na sua aplicação de sistemas de pensamento, pois direciona o entendimento da modelagem a partir da sua compreensão, observando todos os afetados e envolvidos. A noção de caixa-preta trata a organização enquanto um sistema, cuja função de transferência, ou mecânica interna, só pode ser compreendida pela observação do sistema a partir de fora para dentro e por consequencia, a construção de evidências sobre como usar ou controlar o sistema. A noção de teste de caixa-branca, no entanto, leva a uma engenharia por meio de uma orientação de dentro para fora da organização, onde a realização da abordagem não é apenas operacional, mas transformacional, com a preocupação de construir e mudar a organização [**9**] [**16**].

Para Dietz, isto é possível por meio da construção de uma ontologia da empresa e de planos formais sobre função da organização de transferência, estrutura e composição. As organizações precisam ser do tipo caixa branca, a fim de melhorar sistematicamente sua transferência de funcionalidades. Assim, o processo de transformação pode ser articulado, principalmente como um processo incremental de construção de análise e engenharia de modelos. Somente, desta forma, a implementação do sistema de uma organização, no contexto deste trabalho e da arquitetura corporativa desejada[2] será redesenhada e melhorada [**16**].

2.2 CONCEPÇÕES SISTÊMICAS EM ORGANIZAÇÕES SOCIAIS

De acordo com Valença nas pesquisas sobre dinâmica de sistemas, os arquétipos sistêmicos foram criados como modelos de leitura ou de compreensões de uma situação que podem ser usadas tanto em casos específicos quanto na generalidade de casos

[2] A arquitetura corporativa desejada prega que a gestão e a governança de TI trabalham ao mesmo tempo, com arquitetura de negócio e arquitetura estratégica, as quais visam o alinhamento organizacional. Arquitetura corporativa desejada representa uma etapa do ciclo de gestão e governança responsável por propor melhorias à arquitetura corporativa envolvendo estratégia e tomada de decisão em todos os níveis de desempenho. Esse assunto tem uma abordagem ampla nos capítulos 3 e 4 do presente trabalho.

semelhantes, porque nestes últimos se repete um padrão de estruturas dinâmicas de causalidade [**17**]. São combinações ou construções de determinados padrões de inter-relações de causalidade entre variáveis que revelam uma estrutura dinâmica, mas com uma característica notável: são estruturas pouco percebidas a primeira vista, embora frequentes e comuns em situações semelhantes.

Em um sentido vasto, a dinâmica de sistemas tem por objetivo a compreensão sobre como os objetos de um sistema interagem entre si, pois tanto os objetos quanto as pessoas em um sistema interagem através de laços de realimentação e demonstram como uma mudança em uma variável afeta outras variáveis.

Valença defende que o entendimento acerca do pensamento sistêmico enquanto capacidade de conhecimento do ambiente e previsão das consequências de uma ação pelo encadeamento e dependências existentes [**17**]. Segundo Kasper, a apresentação do pensamento sistêmico se dá como forma de ver e falar sobre a realidade, que nos auxilia a entender e trabalhar melhor com sistemas para influenciar a qualidade de vida [**18**].

O pensamento analítico lida com os conjuntos independentes de variáveis, assumindo que a estrutura é suficiente para compreender um sistema. O pensamento sintético trata o entendimento do todo, do ponto de vista do resultado. Ou seja, o tratamento conjunto das variáveis independentes. Dessa forma, para Gharajedaghi a eficiência de uma abordagem de sistemas reside na interação, por meio da observação dos seguintes fundamentos do pensamento sistêmico: Pensamento holístico (iteração da função, estrutura e processo); Pensamento Operacional (dinâmica de vários ciclos - *multi-loop*, sistemas de *feedback*; caos e complexidade); Auto-organização, movimento em direção a uma ordem pré-definida (modelo sócio-cultural); Design interativo (redesenhar o futuro e inventar maneiras de realizá-lo), conforme demonstra a Figura 2.1 [**19**].

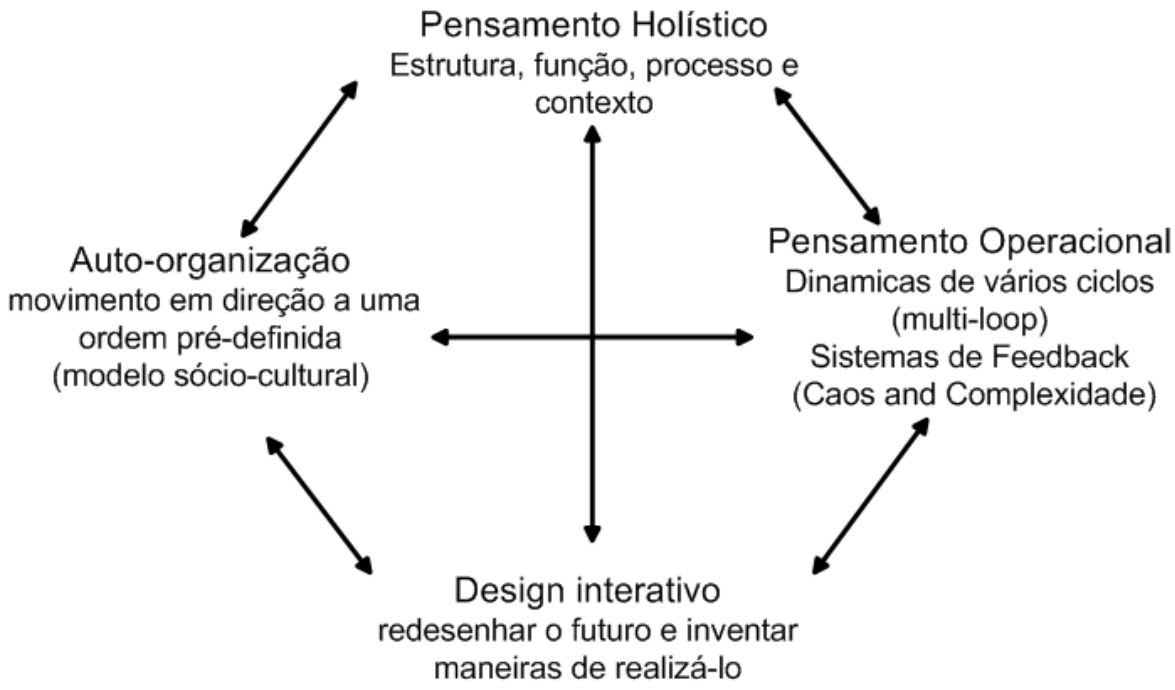


Figura 2.1 - As quatro fundações e uma abordagem por sistemas
Fonte: [**19**]

A utilização de uma abordagem por meio do design interativo e a interação entre funcionalidade, estrutura e processos, quando combinados com o pensamento operacional acrescido da compreensão das implicações para o comportamento de auto-organização, é responsável por desenvolver um sistema competente suficientemente para lidar com os desafios emergentes dos sistemas sociais [**19**].

O pensamento sistêmico demonstra que um processo referente a um grupo organizado de tarefas relacionadas e atividades que trabalham em conjunto para transformar entradas em saídas que criam um valor para os *stakeholders*, conforme Gharajedaghi . Um processo pode incluir quaisquer papéis, responsabilidades, ferramentas e controles gerenciais fundamentais para entrega do resultado esperado de maneira confiável. Um processo pode definir políticas, normas, recomendações, atividades e instruções de trabalho caso sejam necessários. A funcionalidade descreve as saídas ou resultados produzidos e a estrutura é definida pelos componentes e os seus relacionamentos existentes dentro de uma organização.

Para Lankhorst as organizações que possuem alinhamento entre TI e Negócio são constantemente beneficiadas com a efetividade organizacional, que não é só percebida em

áreas isoladas mas também em toda a organização [**20**]. Assim, a arquitetura fornece um meio para lidar com a complexidade da informação nas organizações. Para este fim, os arquitetos corporativos precisam expressar de forma mais clara possível as arquiteturas corporativas, tanto para sua própria compreensão quanto para a comunicação com outros *stakeholders*, tais como os desenvolvedores do sistema, os usuários finais ou gestores.

O conceito de serviços desempenha um papel central na modelagem organizacional, conforme Lankhorst. Um serviço é definido como uma unidade de funcionalidade, com a geração de valor para entidades específicas, por exemplo: um sistema, organização ou departamento. O serviço orientado pode levar a visão em camadas de modelos de arquitetura corporativa, onde o conceito de serviço é o principal elo entre as diferentes camadas [**20**].

As camadas de serviços com serviços disponibilizados para as camadas mais altas são intercaladas com camadas de implementação que realizam os serviços, conforme demonstra a Figura 2.2. Assim, dentro de uma camada pode haver, também, serviços internos. Tal fator estrutura uma pilha de camadas e estas camadas de serviço de implementação são ligadas por relações. Estas relações exibem como as camadas de aplicação podem fazer uso dos serviços de outras camadas, normalmente as camadas inferiores, e aponta como os serviços são realizados em uma camada de aplicação.

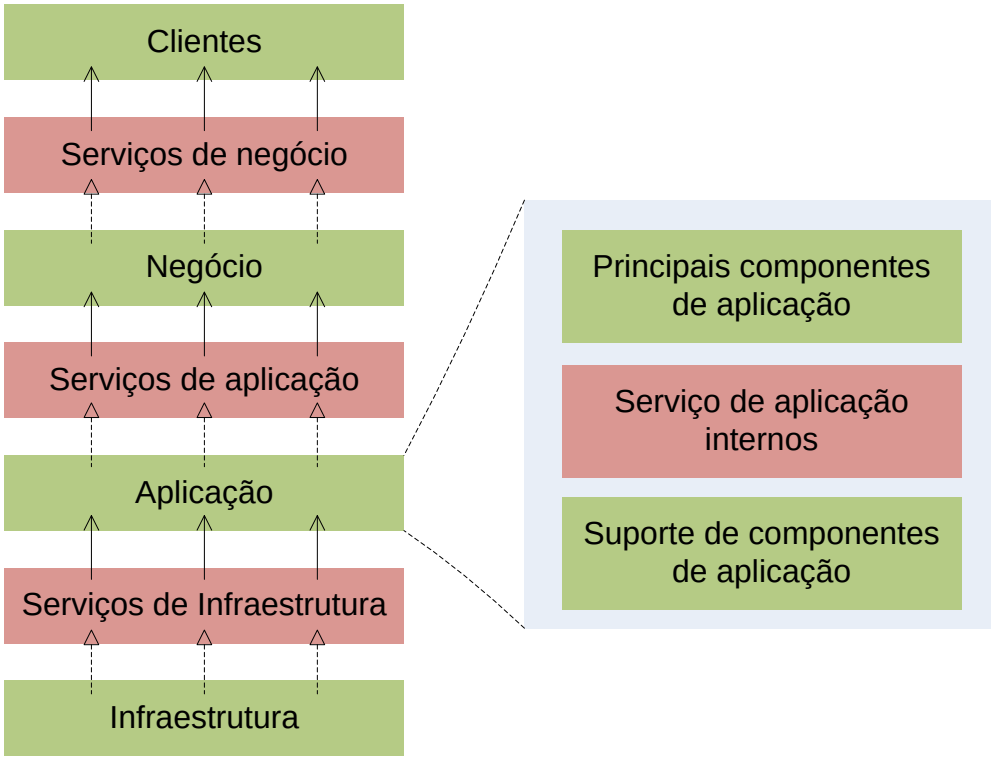


Figura 2.2 - Visão por camadas de funcionalidade
Fonte: [**20**]

Embora, em um nível abstrato, os conceitos utilizados dentro de cada camada são semelhantes, conceitos mais concretos e específicos para uma determinada camada são definidos de acordo com Lankhorst.

- A camada de negócios oferece produtos e serviços para clientes externos, que são desenvolvidos na organização por processos de negócios;
- A camada de aplicação apoia a camada de negócios com serviços de aplicativos que são realizadas por componentes (*software*) aplicativos;
- A camada de infraestrutura técnica oferece serviços de infraestrutura, ,por exemplo, serviço de armazenamento, processamento e comunicação necessários para executar o aplicativo. Realizado por computador e por dispositivos de comunicação e *software* do sistema.

O modelo de arquitetura corporativa de TI, por meio de uma visão das funcionalidades, representado pelo conceito de configurações de valor e apoiado pelo pensamento sistemico descreve a organização de TI por subsistemas. Os subsistemas de

uma organização são como a entidade responsável por prestar todos os serviços de TI às outras entidades da organização de tal forma que os subsistemas de TI são organizados em três subsistemas lógicos, que interagem entre si e permitem o alinhamento entre a TI e o negócio, denominados Direcionamento, Desenvolvimento e Entrega [**21**].

A compreensão de um modelo que descreva o comportamento dinâmico de uma área de TI facilita a busca pela excelência das funcionalidades desejadas e, consequentemente, os resultados alcançados. Além disso, devem-se considerar os requisitos não funcionais que suportam a maioria dos objetivos de qualidade de um ambiente de TI, quais sejam [**21**]:

- Velocidade de resposta de implantação das mudanças orientadas pelos consumidores ou pelas estratégias;
- Eficácia, eficiência e transparência de custos;
- Gerenciamento de riscos efetivos;
- Eficácia operacional.

Assim, observa-se que a visão de funcionalidades de cada atividade dentro do subsistema atravessa as fronteiras teóricas gerando uma sobreposição. E, de acordo com Molinaro *apud* Betz, devem-se considerar as seguintes questões [**4**] [**22**]:

- Perspectiva de planejamento e controle de alto nível – Direcionamento;
  - Quais são os investimentos futuros mais promissores no portfólio de TI?
  - Quais os investimentos correntes são bons? Questionáveis? Ruins?
  - Para uma aplicação ou serviço, quais são os custos totais de aquisição e operação?
- Perspectiva da construção de soluções – Desenvolvimento;
  - É preciso melhorar um serviço ou sistema?
    - Qual é a lista completa de recursos?
    - Quais são as interdependências e as suas naturezas?
  - Que sistemas usam um determinado elemento de dados?
    - Qual o significado destes dados em cada uma das situações?
    - Quais as políticas de segurança e privacidade que se aplicam a estes dados?

- Qual o nível corrente de mudanças nos meus sistemas?

- Perspectiva operacional – Entrega;
  - Como é o consumo de recursos?
    - Na construção de soluções?
    - Na operação e manutenção?
  - Qual o status operacional e tendências dos sistemas?
    - No número de incidentes e problemas?
    - No esforço em suporte e manutenção?
    - Na quantidade de mudanças?
  - Como as métricas de incidentes e problemas se relacionam com as atividades de mudança?

A proposta da presente dissertação considera os conceitos de funcionalidade apresentados, sob o ponto de vista da organização, como uma visão sistêmica, capaz de agregar suas definições de maneira a explorar suas aplicações e estabelecer, para um mesmo conceito. Tal fator permite que as relações sejam definidas com clareza e o papel organizacional aplicado em qualquer contexto que se deseja analisar.

2.3 GOVERNANÇA CORPORATIVA

O termo governança corporativa foi criado no início da década de 1990 para definir as regras que regem o relacionamento dentro de uma companhia dos interesses de acionistas controladores, acionistas minoritários e administradores [**23**] [**24**]. A governança corporativa tornou-se um tema dominante nos negócios por ocasião dos escândalos corporativos ocorridos em meados de 2002. A gravidade dos impactos financeiros desses escândalos abalou a confiança de investidores tanto institucionais quanto individuais e aumentou a preocupação com a habilidade e a determinação das empresas privadas de proteger seus *stakeholders*[3] [**23**]. Segundo Weill, uma boa governança corporativa é importante para os investidores profissionais. Grandes instituições atribuem à governança

[3] Os *stakeholders* são todos os envolvidos com a companhia, como clientes, empregados, fornecedores, etc.

corporativa o mesmo peso que aos indicadores financeiros quando avaliam decisões de investimento [**14**].

A governança corporativa é um sistema por meio do qual as organizações podem ser dirigidas e monitoradas. O sistema de governança permite que a missão, a visão e a estratégia sejam transformadas tendo em vista os resultados desejados. A dependência da organização das ferramentas de informação é muito grande, e as questões de governança não podem ser resolvidas sem o uso intensivo da tecnologia da informação [**4**].

Governança corporativa é definida por Garcia como a regulamentação da estrutura administrativa da sociedade anônima, através do estabelecimento dos direitos e dos deveres dos vários acionistas e da dinâmica e organização dos poderes [**23**]. Seu principal objetivo é recuperar e garantir a confiabilidade em uma determinada empresa para seus acionistas, criando um conjunto eficiente de mecanismos, tanto de incentivos quanto de monitoramento, a fim de assegurar que o comportamento dos executivos esteja sempre alinhado com o interesse dos acionistas.

Governança corporativa pode ser definida pelo IBGC como um sistema que assegura aos sócios-proprietários o governo estratégico da empresa e o efetivo monitoramento da diretoria executiva [**25**]. A relação entre propriedade e gestão se dá por meio do conselho de administração, a auditoria independente e o conselho fiscal, instrumentos fundamentais para o exercício do controle. A boa governança assegura aos sócios equidade, transparência, responsabilidade pelos resultados (*accountability*) e obediência às leis do país (*compliance*).

A prática da governança corporativa deve fazer com que a organização siga determinadas normas instituídas e seja transparente com seus funcionários e acionista de forma a prover à eficácia e eficiência organizacional. O presente trabalho utiliza-se da conceituação de governança corporativa como um conjunto de práticas, regras, costumes, leis, políticas e regulamentos que tem como finalidade regular o modo como uma empresa é administrada e controlada, favorecendo os interesses de acionistas, administradores, funcionários e fornecedores. Desta forma, auxilia no entendimento dos processos organizacionais bem como no entendimento da condição de existência e papeis da organização.

2.3.1 Arquitetura corporativa

O conceito de Tecnologia da Informação, conforme Buss pode ser entendido como, "a integração dos seus dois termos: Tecnologia e Informação. A TI envolve os recursos tecnológicos de *hardware*, *software*, telecomunicações, automações, multimídia, armazenamento de dados, serviços de suporte, entre outros" [**26**]. Todos esses recursos voltados ao gerenciamento da informação e a presença da TI em quase todos os tipos de operações, além do ritmo intenso do desenvolvimento tecnológico faz com que esta área se torne fundamental às organizações [**27**].

A arquitetura corporativa pode ser entendida como a lógica organizadora de processos de negócio e de recursos de Tecnologia da Informação que reflete os requisitos de integração e de padronização do modelo operacional de uma empresa. Assim, a informação é reconhecida pelas organizações como um dos mais importantes recursos estratégicos que necessitam de gerenciamento [**14**].

Para Molinaro, a arquitetura corporativa consiste em um todo coerente de princípios, métodos e modelos que são usados no projeto e na realização de uma estrutura organizacional, processos de negócio, sistema de informação e infraestrutura tecnológica [**4**]. A comunicação entre os elementos essenciais que explicam o funcionamento de uma organização em conjunto com as partes interessadas descreve o papel da arquitetura corporativa, pois permite a seus gestores a obtenção de uma ideia clara dos pontos que devem ser tratados para atingir as metas desejadas.

As arquiteturas corporativas exploram continuamente como as tecnologias da informação apóiam e melhoram a aprendizagem organizacional e a incorporação permanente de conhecimento, auxiliando os gestores na tomada de decisão. Um dos principais meios para visualização do funcionamento sistêmico da organização é através do entendimento da arquitetura corporativa e este entendimento pode ser posto em prática com o uso dos frameworks de arquitetura corporativa [**22**].

Para a visualização do funcionamento sistêmico da organização, a arquitetura corporativa pode ser dos principais meios e seu conceito posto em prática com o uso dos frameworks de arquitetura corporativa, pois é por meio das arquiteturas corporativas que a Tecnologia da Informação apoia e melhora a aprendizagem organizacional e a

incorporação permanente de conhecimento, auxiliando os gestores na tomada de decisão [**4**].

A arquitetura de TI, segundo Torres *apud* Buss, pode ser entendida como o conjunto de elementos constituintes da TI. A necessidade e o papel de TI na empresa constituem os fatores determinantes da arquitetura de TI. A função da TI dentro da empresa deve ser derivada da função macro do negócio, onde a sinergia entre a tecnologia e negócio é a chave do sucesso. Para obter esta sinergia, é importante analisar as forças atuantes sobre a arquitetura de TI e como elas afetarão o processo de mudança. A Figura 2.3 apresenta esquematicamente o conceito básico da integração dos negócios à Arquitetura de Informação [**28**] [**26**].

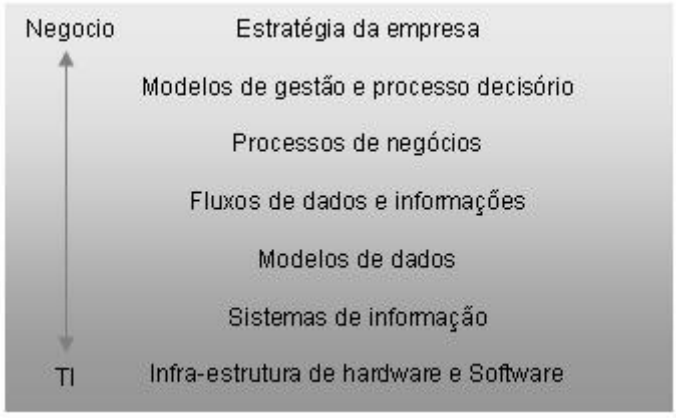


Figura 2.3 - Integração dos negócios com a arquitetura de TI
Fonte: [**26**]

A arquitetura de TI engloba os seguintes componentes:

- Infraestrutura de *hardware* (postos de trabalho e servidores);
- Infraestrutura de comunicação (redes de comunicação e equipamentos);
- Sistemas de informação;
- Sistemas de bancos de dados;
- Metodologias (processos).

De acordo com Molinaro, o desenho da arquitetura corporativa tem como objetivo criar um mecanismo de comunicação comum entre os gestores e técnicos do negócio e os gestores e técnicos de TI, assim como mostrar demonstrar que TI pode apoiar o negócio,

com foco estratégico. O funcionamento da organização do ponto de vista estratégico pode ser estruturado a partir do desenho da arquitetura corporativa, o que facilita a troca de informações entre os gestores e técnicos de negócio e TI. Cada organização deverá ter uma arquitetura única, que será construída e atualizada ao longo do tempo [**4**].

A utilização dos conceitos relativos a arquitetura corporativa neste trabalho visa não só a sua compreensão da definição; bem como, entender a importância de um desenho arquitetural corporativo pois a partir dele as partes interessadas obtem uma ideia clara dos assuntos que devem ser debatidos para atingir os objetivos desejados e, finalmente, descrever o funcionamento da organização em conjunto com os envolvidos.

2.3.2 Governança corporativa de TI

Governança de TI é definida em Weill e Ross, como a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização da TI [**14**]. A administração é o processo de tomar e implementar decisões. Nesse contexto, a governança corporativa determina quem tem o direito de decidir sobre quanto será investido em TI. A Governança trata ainda dos atores responsáveis pela tomada de decisão. A alta gerência estabelece os direitos decisórios e a responsabilidade pela TI para estimular os comportamentos desejáveis na empresa [**14**] [**24**].

Torres descreve que, para a tomada de decisões é necessário que haja informações, controles, processos e procedimentos. Todo um *framework* de responsabilidades para estimular comportamentos desejáveis na utilização de TI. Quanto mais rápida e precisa for à informação, mais eficaz é a gestão e o direcionamento da área de TI e do negócio para o sucesso. Todos estes controles, também estimulam a transparência das instituições para com os seus investidores, mostrando a real aplicação dos valores e o retorno esperado [**28**] [**14**].

De acordo com o *IT Governance Institute*, a governança de TI é responsabilidade da alta administração incluindo, diretores e executivos na liderança e nas estruturas organizacionais e nos processos que garantam que a TI da empresa sustenta e estenda as estratégias e os objetivos da organização. A governança de TI é uma parte integral da Governança Corporativa e é formada pela liderança, estruturas organizacionais e processos

que garantem que a TI sustenta e melhora a estratégia e objetivos da organização [**29**]. A governança de TI está intimamente ligada à responsabilidade dos executivos no que consiste à liderança, à estrutura e processos organizacionais que asseguram a sustentação das estratégias da organização e seus objetivos pela TI [**14**]. Segundo Magalhães, a governança de TI está fundamentada basicamente em pessoas, processos e tecnologia [**30**].

Conforme descrito em Torres *apud* Júnior, a alta direção possui algumas responsabilidades como, assegurar o alinhamento entre a estratégia de TI e a estratégia de negócios e direcionar a execução da estratégia de TI. Na prática, isso funciona por meio do processo de tomada de decisão sobre priorização de investimentos e alocação de recursos; bem como somado a isso, elenca-se ainda, o cumprimento da estratégia de TI por meio de diretrizes claras, indicadores e metas objetivas e, por último, promove uma cultura de abertura e colaboração entre as áreas de negócios e de TI [**28**] [**31**].

A governança corporativa de TI define alguns princípios básicos: objetivos de negócios requerem informações, estas devem atender aos critérios de qualidade, segurança e confiabilidade; informações são produzidas por recursos de TI (dados, aplicações, infraestrutura e pessoas); recursos de TI são gerenciados por processos e estes devem ser controlados por meio de objetivos de controle, indicadores de desempenho e indicadores de resultados [**14**][**24**].

2.3.3 Gerenciamento de TI

Gestão, como descreve Lameira, é um conjunto de regras, estruturas e ações que modelam a execução das funções de uma dada organização. Assim, orienta que uma importante tendência é administrar as organizações enquanto conjuntos de processos interligados e não como conjuntos de departamentos independentes [**32**]. Um modelo de gestão é uma forma simplificada de demonstrar as práticas gerenciais utilizadas pela organização para atingir seus objetivos [**26**]. A administração por processos consiste em administrar as funções permanentes como elos de uma corrente e não como departamentos isolados uns dos outros.

As novas realidades de negócios, de modo geral apontam para empresas fortemente suportadas pela TI. A obtenção de informações precisas, ágeis e confiáveis fez

com que houvesse um aumento considerável sobre as exigências por serviços da TI com qualidade. Em consequência disto a infraestrutura de TI torna-se cada vez mais complexa para suportar todos os processos de negócio [**30**].

A TI é uma das áreas que mais proporcionam valor ao negocio. Assim, um ambiente estável, com as funcionalidades certas, características técnicas adequadas e serviços que suportem os processos de negócio é o que uma área de TI apropriada deve prover à empresa [**33**]. Assim, serviço é algo vital para qualquer empresa, seja ela de pequeno, médio ou grande porte e que reflita a percepção do cliente quanto à qualidade [**30**] [**27**] [**34**]. O conceito de serviço integra vários elementos da organização, sendo caracterizado pela intangibilidade. Pela heterogeneidade, o conceito de serviço é visto que a percepção do cliente sobre a qualidade é variável, pois um serviço pode ser realizado por pessoas diferentes e para clientes diferentes, refletindo padrões distintos de comportamento. Os serviços são consumidos no momento em que são produzidos e o cliente está presente no processo produtivo, refletindo, assim, o comportamento do fornecedor perante o cliente que é parte do processo [**27**] [**34**].

O gerenciamento de serviços em TI utiliza métodos padronizados e pautados pelas necessidades estratégicas das organizações. A multiplicidade de modelos disponíveis atesta a necessidade e importância do gerenciamento da TI. A gestão de serviços de TI, quando bem concebida pode trazer melhorias efetivas para a qualidade dos serviços [**35**]**.** Ao favorecer a comunicação entre a TI e os negócios, a gestão de serviços de TI possibilita retornos mensuráveis sobre os resultados de suas operações. Dessa forma a TI não se coloca mais como geradora de despesas, mas como parceira fundamental na geração de valor ao negócio [**30**] [**35**].

O gerenciamento de serviços de TI é o instrumento pelo qual pode iniciar a adoção de uma postura proativa em relação ao atendimento das necessidades da organização, contribuindo, sobremaneira, à geração de valor. A qualidade dos serviços de TI só poderá ser percebida pelos usuários através das entregas dos serviços de TI atendendo as expectativas geradas. Para alcançar esse objetivo é adotada a implementação do gerenciamento dos processos internos da área de TI [**30**]. Utilizar as práticas já conhecidas e aceitas no mercado para gerenciar a entrega de serviços em TI torna-se uma maneira para proporcionar qualidade esperada. A fim de conquistar e manter as expectativas não só das

organizações, mas também, dos clientes, foi desenvolvido algumas metodologias como: COBIT[4], ITIL[5], BSC[6], ISO, CMMI[7] entre outros. No escopo deste trabalho, as metodologias para controle abordadas serão: ISO/IEC 27001 e 27002.

Um processo de negócio, segundo Azevedo, é uma série de atividades inter-relacionadas que cruza as fronteiras funcionais das empresas com entradas e saídas bem definidas [**36**]. Nascida de uma visão diferenciada em relação aos recursos oferecidos, a TI passou a exercer um papel estratégico dentro das empresas, o processamento dos dados foi criado para dar suporte ao processo de tomada de decisão [**37**]. Sistemas de apoio à gestão fazem parte da infraestrutura necessária para disponibilizar informações à gestão de negócios [**38**].

O cenário administrativo das organizações tem sofrido profundas mudanças ao longo das últimas décadas. Dois conceitos, especialmente, marcaram as recentes transformações na ideologia empresarial: o primeiro, que causou um grande impacto nas empresas durante a década passada, foi o conceito de processos de negócio, em substituição à visão departamental que até então prevalecia. O segundo, atualmente em processo de adaptação nas organizações, é o conceito de gestão colaborativa [**36**].

O gerenciamento de serviços de TI baseia-se em processos. Cada um deles é constituído por um conjunto de atividades inter-relacionadas. A partir de um objetivo estipulado cada processo é executado para atingir os resultados desejados. Um processo não deve ser visto isoladamente, mas para cada processo existe um método de gerenciamento específico e este não deve ser visto isoladamente dos outros processos pela

[4] *Control Objectives for Information and related Technology* (COBIT) (é um guia de boas práticas apresentado como framework, dirigido à gestão de tecnologia de informação (TI). Agrega recursos que podem servir como um modelo de referência para gestão da TI, incluindo um sumário executivo, um framework, objetivos de controle, mapas de auditoria, ferramentas para a sua implementação e principalmente, um guia com técnicas de gerenciamento.

[5] *Information Technology Infrastructure Library* (ITIL) é um conjunto de boas práticas a serem aplicadas na infraestrutura, operação e manutenção de serviços de TI. Busca promover a gestão com foco no cliente e na qualidade dos serviços de TI.

[6] *Balanced Scorecard* (BSC) é uma metodologia de medição e gestão de desempenho. Seus métodos são utilizados na gestão do negócio, nos serviços e na infraestrutura e baseiam-se em metodologias consagradas que podem utilizar a TI e os *softwares* de ERP como soluções de apoio, relacionando-a a gerência de serviços e a garantia de resultados ao negócio.

[7] *Capability Maturity Model Integration* (CMMI) é um modelo de referência que contém práticas (genéricas ou específicas) necessárias à maturidade em disciplinas específicas (*Systems Engineering (SE), Software Engineering (SW), Integrated Product and Process Development (IPPD), Supplier Sourcing (SS)).* O CMMI procura estabelecer um modelo único para o processo de melhoria corporativo, integrando diferentes modelos e disciplinas.

sua inter-relação. A razão pela qual o gerenciamento de serviços de TI é necessária advém da necessidade de ter uma coordenação de todos os processos de TI para obtenção de um objetivo comum [**30**].

2.4 NORMAS ISO/IEC 27001 e NBR ISO/IEC 27002

A norma NBR ISO/IEC 27002, antiga NBR ISO/IEC 17799, é derivada da norma britânica BS 7799. A BS 7799 foi a primeira norma com foco em Sistemas de Informação (SI) e foi desenvolvida pelo *British Standard Institute* (BSI). A primeira parte dessa norma (BS 7799-1) foi publicada em 1995 como um código de melhores práticas de SI. A segunda parte (BS 7799-2), publicada em 1998, de forma geral, implementa o sistema de gestão dessas melhores práticas [**39**].

Em 2000, a BS 7799-1 foi republicada com seu código de melhores práticas atualizado e se tornou uma norma ISO, sendo publicada como ISO 17799:2000. Em 2001, foi publicada no Brasil a primeira versão brasileira dessa norma, sob o nome de NBR ISO 17799. Em 2005, houve várias publicações referentes a essa norma: foi publicada a segunda versão da norma no Brasil (NBR ISO/IEC 17799); a segunda parte da norma BS 7799 se tornou um padrão ISO, a ISO 27001; e a norma ISO 17799:2005 se tornou o padrão ISO 27002. Como várias organizações do mundo inteiro seguem esta norma, criou-se uma base comum para a prática de SI. No Brasil, a norma é referendada pela ABNT com o nome NBR ISO/IEC 27002 [**40**] [**41**].

A norma ISO/IEC 27001 descreve um ativo como algo que agrega valor a uma organização. Ativos de informação estão sujeitos a uma ampla gama de ameaças, tanto externas quanto internas, que vão desde ações aleatórias até ações altamente específicas. Os riscos incluem atos de natureza, fraude ou outras atividades criminosas, erro do usuário e falhas no sistema.

As informações de risco podem ter efeito em um ou mais dos três atributos fundamentais de um ativo de informação. A norma ISO/IEC 27001 define os três atributos fundamentais como:

- Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada, que permite a possibilidade que as informações sejam acessadas por programas de *software*, bem como usuários humanos;
- Confidencialidade: propriedade que a informação não é disponibilizada ou divulgada a indivíduos não autorizados, entidades ou processos;
- Integridade: propriedade de salvaguardar com exatidão e integridade os ativos.

Assim, a Associação Brasileira de Normas Técnicas (NBR) define da segurança da informação como a preservação da confidencialidade, integridade e disponibilidade da informação além de outras propriedades, tais como autenticidade, não repúdio, responsabilidade e confiabilidade podem também estar envolvidas, conforme descrito pela Figura 2.4 [**40**].

Figura 2.4 - Atributos da informação de ativos
Fonte: [**42**]

A norma ISO/IEC 27001 foi preparada para prover um modelo responsável por estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) com base em uma abordagem de risco do negócio, de maneira que o sistema de gerenciamento deve incluir a estrutura organizacional , políticas, planejamento de atividades, responsabilidades, práticas, procedimentos, processos e recursos [**42**].

A adoção de um SGSI deve ser uma decisão estratégica para uma organização dado que as informações e os processos, sistemas e rede que lhes dão suporte são ativos importantes para o negócio. A confidencialidade, a integridade e a disponibilidade das informações são essenciais à manutenção da competitividade. A concepção e implementação do SGSI deve estar diretamente ligada às necessidades e objetivos da organização, bem como requisitos de segurança, processos empregados,o tamanho e a estrutura da organização. A Figura 2.5 descreve a concepção do SGSI baseado em quatro pontos essenciais de uma organização que devem ser considerados durante a sua elaboração.

Figura 2.5 - Gerenciamento estratégico de risco da informação para um SGSI
Fonte: [**43**]

A norma ISO/IEC 27001 promove a adoção de uma abordagem de processos para a concepção e implantação de um SGSI, que é amplamente conhecida como modelo *Plan-Do-Check-Act*[8] (PDCA). A norma ISO/IEC 27001 carrega consigo uma leitura de como o modelo PDCA deve ser aplicado para a implementação de um SGSI. A introdução da

[8] O modelo *Plan-do-Check-Act* será descrito com mais detalhes no item 2.5.1 deste trabalho.

norma ISO/IEC 27002 descreve este modelo e define como aplicá-la em um ambiente de segurança da informação.

Diante da abordagem para concepção e implantação de um SGSI, as fases do modelo PDCA relacionam-se com as etapas para a realização de um SGSI [**40**] [**43**], conforme descrito na Figura 2.6:

- *Plan*: Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes ao gerenciamento de de riscos e a melhoria da segurança da informação para produção de resultados de acordo com as políticas e objetivos globais da organização;
    - Definir o escopo do SGSI;
    - Definir a política de segurança da informação;
    - Definir uma abordagem sistemática para avaliação dos riscos e aceitação de critérios;
    - Realizar uma avaliação de risco para identificar, dentro do contexto da política e escopo do SGSI, os ativos de informações importantes da organização e os riscos a eles associados;
    - Identificar e avaliar as opções para o tratamento destes riscos, selecionar, quando necessário, os objetivos e a seleção de controles a serem implementados;
    - Preparar uma declaração de aplicabilidade.

- *Do:* Implementar e operar a política, controles, processos e procedimentos do SGSI.
    - Formular um plano de tratamento de riscos e sua documentação, incluindo processos planejados e qualquer documentação de apoio necessária;
    - Implementar o plano de tratamento de riscos e controles planejados;
    - Formar adequadamente o pessoal envolvido, bem como programas de sensibilização;
    - Realizar a gestão de operações e recursos de acordo com o SGSI; Implementar os procedimentos que permitem a detecção imediata e a resposta a incidentes de segurança.

- *Check:* Avaliar e, quando possível, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para análise crítica por parte da direção.
    - Monitorar, revisar, testar e auditar. Considerar que o monitoramento, a revisão, o teste e a auditoria formam um processo contínuo que deve abranger todo o sistema.

- *Act:* Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.
    - Identificar, documentar e implementar processos de melhoria contínua no SGSI.

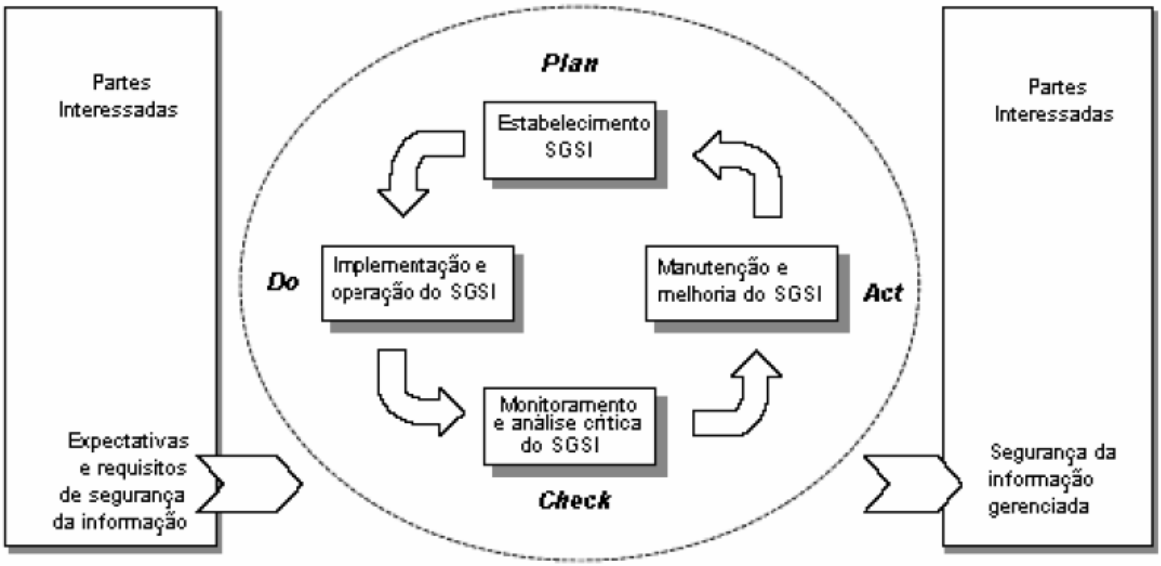


Figura 2.6 - Integração do modelo PDCA com os processo do SGSI.
Fonte: [**40**]

A norma ISO / IEC 27002:2005 descreve um código de boas práticas e se destina a fornecer um quadro das melhores práticas internacionais em segurança da informação, gerenciamento e interoperabilidade de sistemas. Seu objetivo é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização e possibilite critérios de implementação de um SGSI

certificável.

É importante notar que, enquanto a norma ISO/IEC 27002 fornece melhores práticas internacionais em segurança da informação, e neste contexto, a segurança da informação pode ser definida pela proteção de informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio da organização. A norma ISO/IEC 27002 foi escrita especificamente para ser independente de tecnologia e é constituida por 11 seções que tratam especificamente dos controles de segurança da informação e a partir destes controles distribui 133 objetivos de controle que garantem suporte necessário ao desenvolvimento de um SGSI. As seções estão divididas em [**41**]:

- Política de segurança da informação: criação de um documento sobre a política de segurança da informação da organização, que deve conter, entre outros, os conceitos de segurança da informação, o comprometimento da direção com a política, uma estrutura para estabelecer os objetivos de controle e os controles, a estrutura de análise e avaliação e gerenciamento de riscos, as políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização.
- Organizando a Segurança da Informação: estabelecer uma estrutura para gerenciar a organização de forma a coordenar por representantes de diversas partes da organização, com funções e papéis relevantes. Todas as responsabilidades pela segurança da informação. Estabelecer acordos de confidencialidade para proteger as informações de caráter sigiloso, bem como as informações que são acessadas, comunicadas, processadas ou gerenciadas por partes externas, tais como terceiros e clientes.
- Gestão de Ativos: proteger e manter os ativos da organização. Para tanto os ativos devem ser identificados e levantados com proprietários também identificados e designados, de maneira a permitir que o inventário de ativos possa ser estruturado e posteriormente mantido.
- Segurança em recursos humanos: estabelecer critérios para descrever as competências e habilidades necessárias para um cargo e os termos e condições de contratação devem ser explícitos, especialmente no que tange às responsabilidades de segurança da informação para que cada envolvido

entenda suas responsabilidades e esteja de acordo com o papel que desempenhará.

- Segurança física e do ambiente: estabelecer áreas seguras para as instalações de processamento de informação críticas ou sensíveis com níveis e controles de acesso apropriados, incluindo proteção física.
- Gestão das Operações e Comunicações: definir procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações.
- Controle de acesso: controlar o acesso à informação, aos recursos de processamento das informações e aos processos de negócios com base nos requisitos de negócio e na segurança da informação.
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação: identificar os requisitos de segurança de sistemas de informação e definir acordos antes do seu desenvolvimento ou de sua implementação.
- Gestão de Incidentes de Segurança da Informação: estabelecer procedimentos formais de registro e escalonamento para assegurar que eventos de segurança da informação sejam comunicados dentro do menor tempo possível, de tal forma que a tomada de ação corretiva ocorra em tempo hábil.
- Gestão da Continuidade do Negócio: desenvolver planos de continuidade do negócio, incluindo os controles necessários para identificar e reduzir riscos, de forma a assegurar que as operações essenciais sejam rapidamente recuperadas no caso de uma interrupção das atividades. O propósito é proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar que a sua retomada ocorra em tempo hábil.
- Conformidade: Observar o cumprimento as normas, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação a fim de garantir e evitar a violação de qualquer lei criminal ou civil.

2.4.1 Ciclo PDCA enquanto Modelo de Gestão

O ciclo PDCA, como descreve [**44**] [**26**] [**45**] [**32**], pode ser utilizado como um modelo de gestão baseado em processos. Foi desenvolvido na década de 1930 onde planejar (*Plan*), executar (*Do*), controlar (*Check*) e agir (*Act*) formam um ciclo de controle estatístico de processos que sugere a melhoria contínua. O PDCA é aplicado para se atingir resultados dentro de um sistema de gestão e pode ser utilizado em qualquer empresa de forma a garantir o sucesso nos negócios, independentemente da área de atuação da empresa. A Figura 2.7 mostra que, pela aplicação do ciclo PDCA na área de TI é possível atingir um nível de maturidade na organização, consolidando o controle contínuo da qualidade.

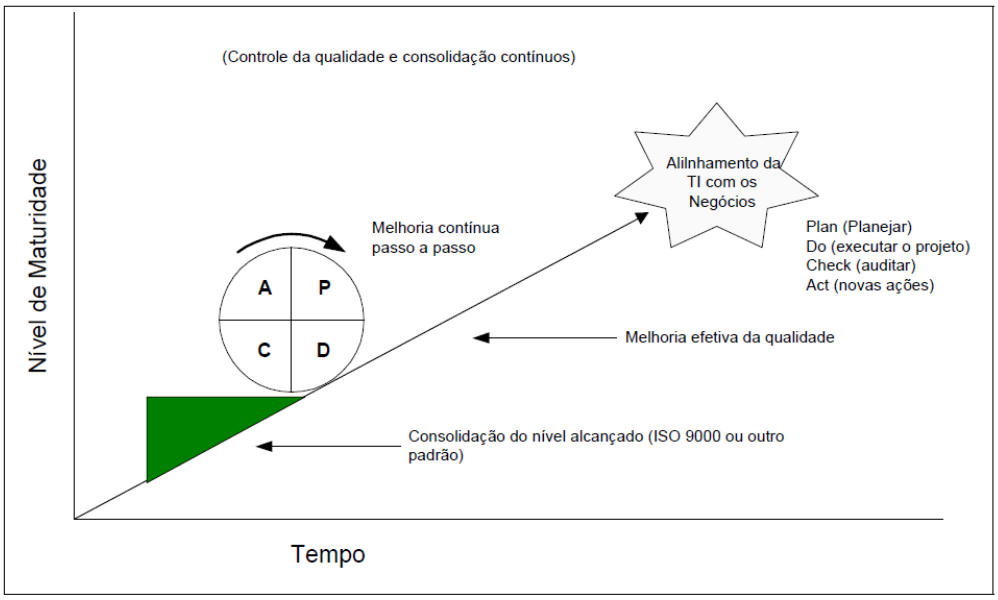


Figura 2.7 - Ciclo PDCA na área de TI
Fonte:[**44**][**28**]

O PDCA consiste em uma seqüência de passos utilizados para controlar qualquer processo definido. É uma ferramenta que auxilia a organização do processo de implementação de melhorias, através de diretrizes claras para a condução de projetos. É também utilizado para o planejamento de testes para obtenção de informações a respeito de um processo, antes da implementação de uma melhoria [**46**].

As fases do ciclo podem ser descritas como:

- *Plan*: Refere-se ao planejamento do seu projeto de melhoria, ou seja, quais são os objetivos, o que se sabe, o que se quer aprender e o irá ser feito (quem, o que, quando, onde, como);
- *Do:* Refere-se à execução do planejamento realizado na fase anterior;
- *Check:* Refere-se à realização de análise dos dados e com base em tal análise verifica quais são as conclusões que podem ser obtidas por meio do processo de coleta de dados;
- *Act:* Refere-se a definição de quais mudanças poderão ser feitas e quais outros ciclos podem ser criados para a melhoria do processo em questão.

O quadro 2.1 descreve um detalhamento de cada fase do ciclo PDCA de forma a permitir a clarificação de suas funcionalidades e o entendimento de sua aplicabilidade quando integrado com as Normas ISO/IEC 27001 e ISO/IEC 27002.

Quadro 2.1 - Fases do ciclo PDCA

Ciclo PDCA Etapa	Detalhamento dos pontos importantes de cada fase
Plan	a) Descrição do Problema – ser capaz de descrever qual o ponto (processo/problema) a suportar o processo de analise crítica no presente ciclo e em linha gerais o que deve ser mantido e melhorado. b) Prognósticos sobre as questões – Descrever as possíveis ocorrências sobre um determinado evento. Para tanto se utiliza de recursos como dados históricos, identificação de vulnerabilidades, ameaças e riscos. c) Desenvolvimento do Plano – Realizar um estudo de planejamento ou da mudança a ser alcançada ou do experimento (teste) a ser executado. O planejamento deve contemplar as ações a serem efetuadas, o período, a descrição do modo de atuação, os responsáveis pelo processo e a localização.
Do	Implementar a execução do planejamento estabelecido na etapa anterior, observando os pontos analisados. No caso de uma alteração de processo prever pontos de checagem para coleta de observações a fim de monitorar aderência ao especificado.

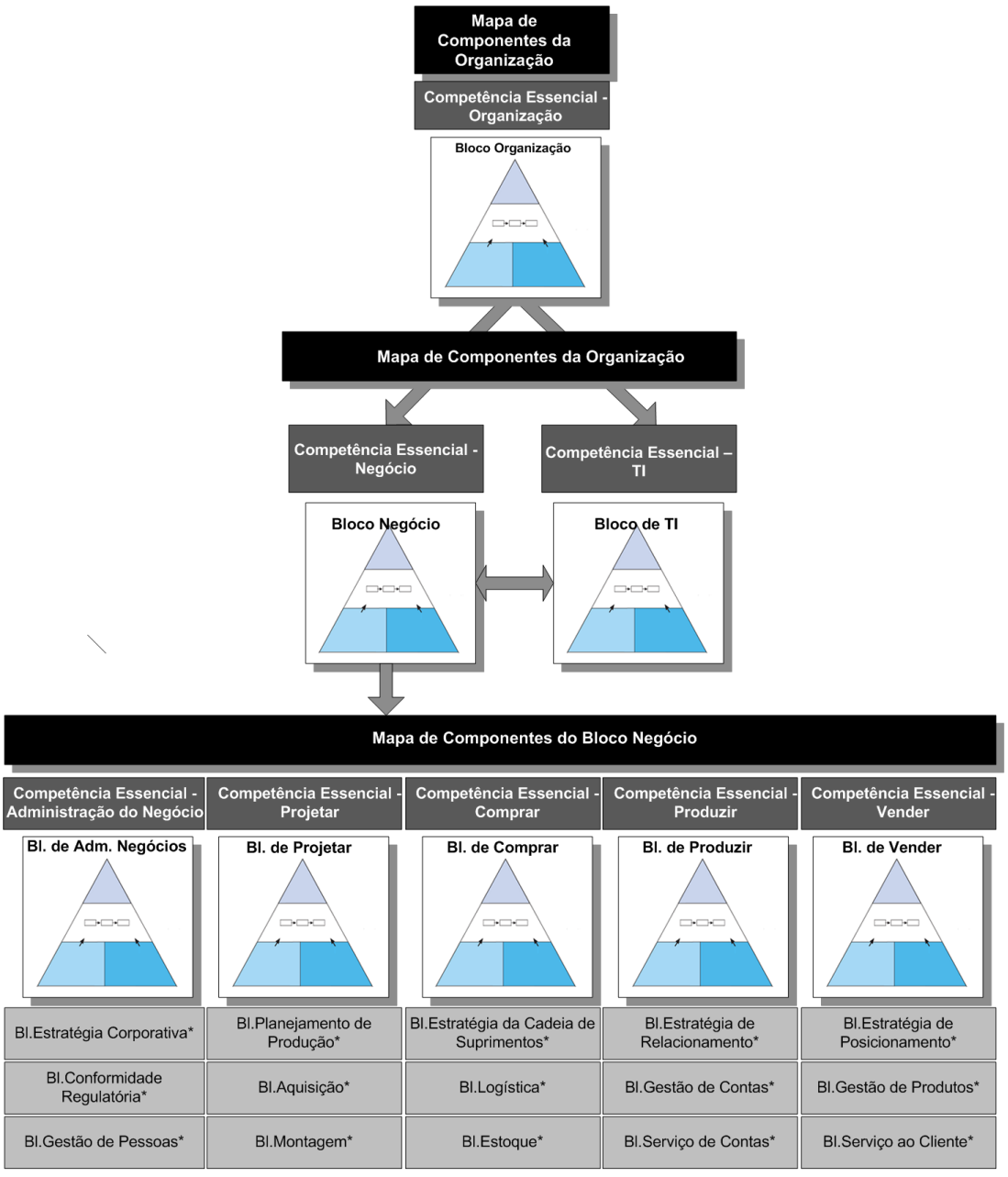
Check	Verificar o aprendizado adquirido durante o cumprimento do plano. A averiguação deve comparar os resultados obtidos com as predições feitas durante o planejamento e, ainda, se observa se os objetivos descritos no plano foram alcançados. É importante que se faça um pequeno resumo (histórico) dos pontos principais do conhecimento adquirido para que o planejamento não se distancie do desejado e, futuramente, possibilite a realização consultas aos registros como forma de orientação para compreender que os pontos secundários planejados não sejam confundidos com os principais.
Act	Nesta etapa é feita a análise crítica do ciclo PDCA e estabelece-se um plano de ação para implementação de posturas que devem ser tomadas após as conclusões obtidas (auditorias internas) com a realização do planejamento. Assim, tanto ações corretivas quanto ações preventivas podem ser estabelecidas. Nesse contexto, as ações podem modificar um processo ou criar um novo que contemple o esperado.

Fonte: [**46**]

O interesse das organizações no conhecimento advém da necessidade de superar desafios, diferenciando-se pelo que sabe e pela forma como conseguem usar esse conhecimento. Com esta visão, o conhecimento torna-se o ativo mais importante das organizações [**32**]. A necessidade de corresponder às expectativas dos clientes e os objetivos organizacionais tornou o aprendizado parte do diferencial competitivo dentro das organizações modernas. Aprender e aperfeiçoar os conceitos de melhoria contínua, as técnicas e práticas de gerenciamento de projetos e ainda construir um sistema de gestão voltado para o constante aprendizado elevou a consciência para a importância dos ativos intangíveis nas organizações.

3 UMA ABORDAGEM PARA INTEGRAÇÃO DA SEGURANÇA NA GESTÃO DE TI SOB O ENFOQUE DAS ISO/IEC 27001 E 27002

Segundo Molinaro as organizações são sistemas formados por componentes que, quando inter-relacionados, coletam, recuperam, processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisão, a coordenação e o controle da organização. Centrada nessa visão, é possível decompor a organização nas seguintes partes: organização, negócio e TI, conforme demonstra a Figura 3.1 [**4**].



**** Componentes do Mapa de Componentes do Bloco Negócio, exemplo de blocos de uma empresa de manufatura, extraído do livro de Sandy Carter (2007).***

Figura 3.1 - Mapa de componentes da organização
Fonte: [**4**]

Assim, um sistema pode ser constituído por outros subsistemas e nesse contexto Betz descreve os subsistemas de uma organização como a entidade responsável pela prestação de todos os serviços de TI às outras entidades da organização de tal forma que os subsistemas de TI são organizados em três subsistemas lógicos, que interagem entre si e permitem o alinhamento entre a TI e o negócio, denominados Direcionamento, Desenvolvimento e Entrega, conforme demonstra a Figura 3.2 [**21**].

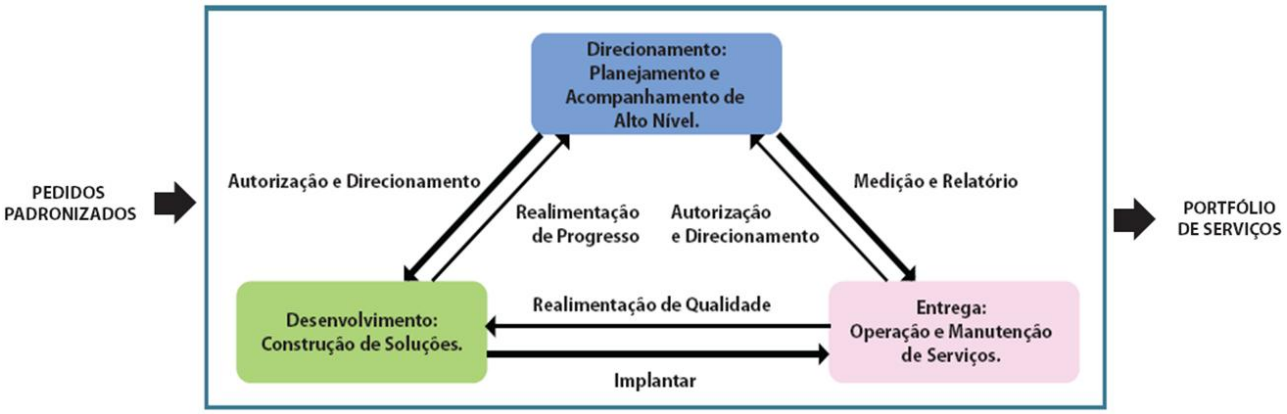


Figura 3.2 - Relacionamento entre sistemas
Fonte: [**21**]

O subsistema Direcionamento está envolvido com o planejamento estratégico da área de TI e sua arquitetura organizacional. As atividades de controle de alto nível estão divididas entre a compreensão, decisão e o monitoramento ações necessárias para o estabelecimento da governança de TI adequada às necessidades da organização unindo, desta forma a TI ao negócio. A funcionalidade essencial do Direcionamento é o planejamento e o controle de alto nível [**4**].

O subsistema Desenvolvimento é o subsistema responsável pelo desenvolvimento dos projetos aprovados pelo subsistema Direcionamento. A funcionalidade essencial do Desenvolvimento consiste em promover a construção de soluções e suas atividades está pautada nos projetos autorizados com as diretrizes de governança determinadas pelo Direcionamento [**4**].

O papel do subsistema Entrega está voltado para operação das atividades do dia a dia de acordo com as diretrizes de governança do Direcionamento e as soluções desenvolvidas pelo Desenvolvimento. Sua principal funcionalidade é a operação e a manutenção de serviços [**4**].

Cada subsistema de TI possui uma característica bem definida a respeito do seu escopo de atuação. No entanto, dentro da dinâmica interna de operacionalização observa-se que os subsistemas se sobrepõem. Ou seja, no subsistema Direcionamento é possível observar além das funcionalidades especificas, partes das funcionalidades pertinentes aos subsistemas Desenvolvimento e do subsistema Entrega. Assim como no subsistema Desenvolvimento, nota-se a presença de funcionalidades referentes aos subsistemas Direcionamento e Entrega. Dessa forma, entende-se que cada subsistema de TI dentro de sua completude de funcionalidade exercerá papéis e irá possuir características referentes aos demais subsistemas em seu escopo de atuação, conforme representado pela Figura 3.3.

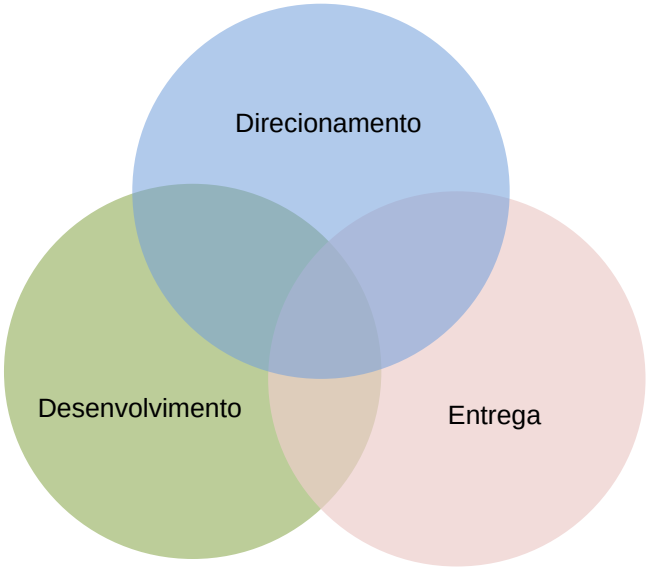


Figura 3.3 – Inter-relacionamento entre Subsistemas de TI
Fonte: [**21**]

A abordagem de integração de segurança a gestão de TI proposto nesta dissertação baseia-se na concepção de organização baseado no modelo de arquitetura corporativa de TI incorporado aos domínios Negócio, Aplicação e Infraestrutura [**21**]. Dessa forma é possível descrever para cada subsistema de TI, descrito pelo modelo de arquitetura corporativa de TI (Direcionamento, Desenvolvimento e Entrega), incorporar os domínios da organização (Negócio, Aplicação e Infraestrutura) com o apoio dos serviços de Negócio, serviços de Aplicação e serviço de Infraestrutura de tal forma que a utilização de uma visão analítica, que observa a organização por suas partes, ou sintética, que analisa a organização por todos os envolvidos, é mediada pelo paradigma de processos, conforme mostrado nas Figura 3.4 e 3.5.

O sistema apoiado pelo trio proposto por [**47**]: funcionalidade, processos e estrutura representa três aspectos que definem um conjunto complementar com a mesma finalidade. A estrutura desenha os componentes e suas relações necessárias para o desenvolvimento dos processos. Os processos descrevem a sequência de acontecimento e as interações dinâmicas necessárias às atividades para produção do resultado proposto a ser alcançado, o qual é definido pela funcionalidade.

Assim, pode-se entender que governar e gerenciar dependem da capacidade de compreender a organização vista tanto como um todo quanto por partes, sendo os processos as atividades que as conectam. Governar está diretamente relacionado à tomada de decisão que toma como base a compreensão das partes, dos processos e das funcionalidades da organização. De forma específica, governar depende da capacidade de compreensão, decisão e monitoramento das ações executadas e definidas na Estrutura, Processos e Funcionalidades.

A partir do entendimento de uma organização considerando os subsistemas de TI, com a aplicação nos domínios (Negócio, Aplicação e Infraestrutura) este trabalho propõe a execução de controles, conforme Figura 3.6, como forma de governar e gerenciar as ações executadas com base no conceito sistêmico de trio: Estruturas, Processos e Funcionalidades das organizações utilizando, para tanto, um conjunto de normas descritas, neste contexto, pela ISO/IEC 27001 e ISO/IEC 27002. Tais normas responsáveis por estabelecer códigos e requisitos de prática para gestão da segurança da informação por meio de padrões internacionais. Estas normas recaem sob a premissa de que a segurança da informação pode ser obtida através da implementação de um conjunto adequado de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software* [**41**].

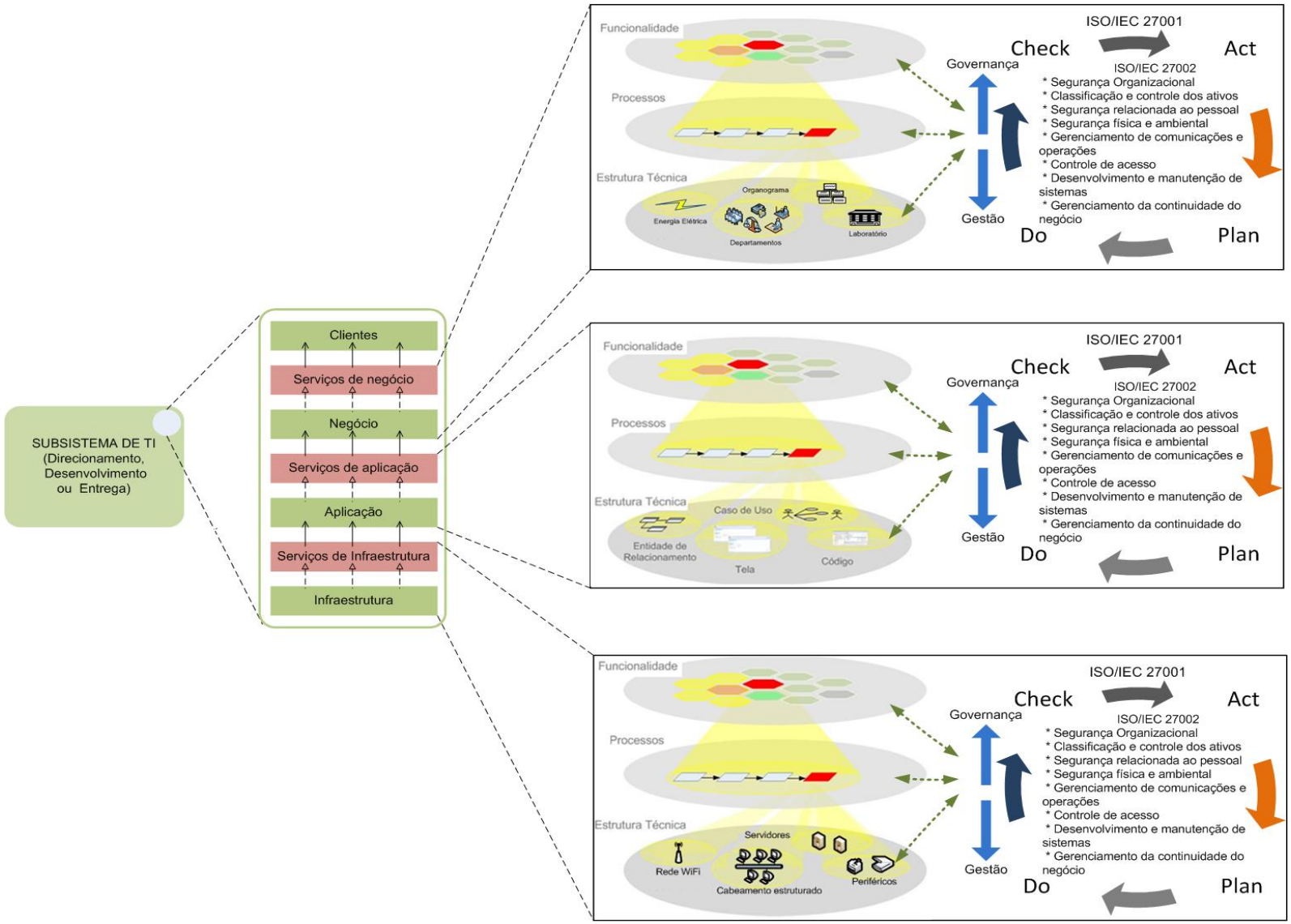


Figura 3.4 - Integração entre os modelos propostos

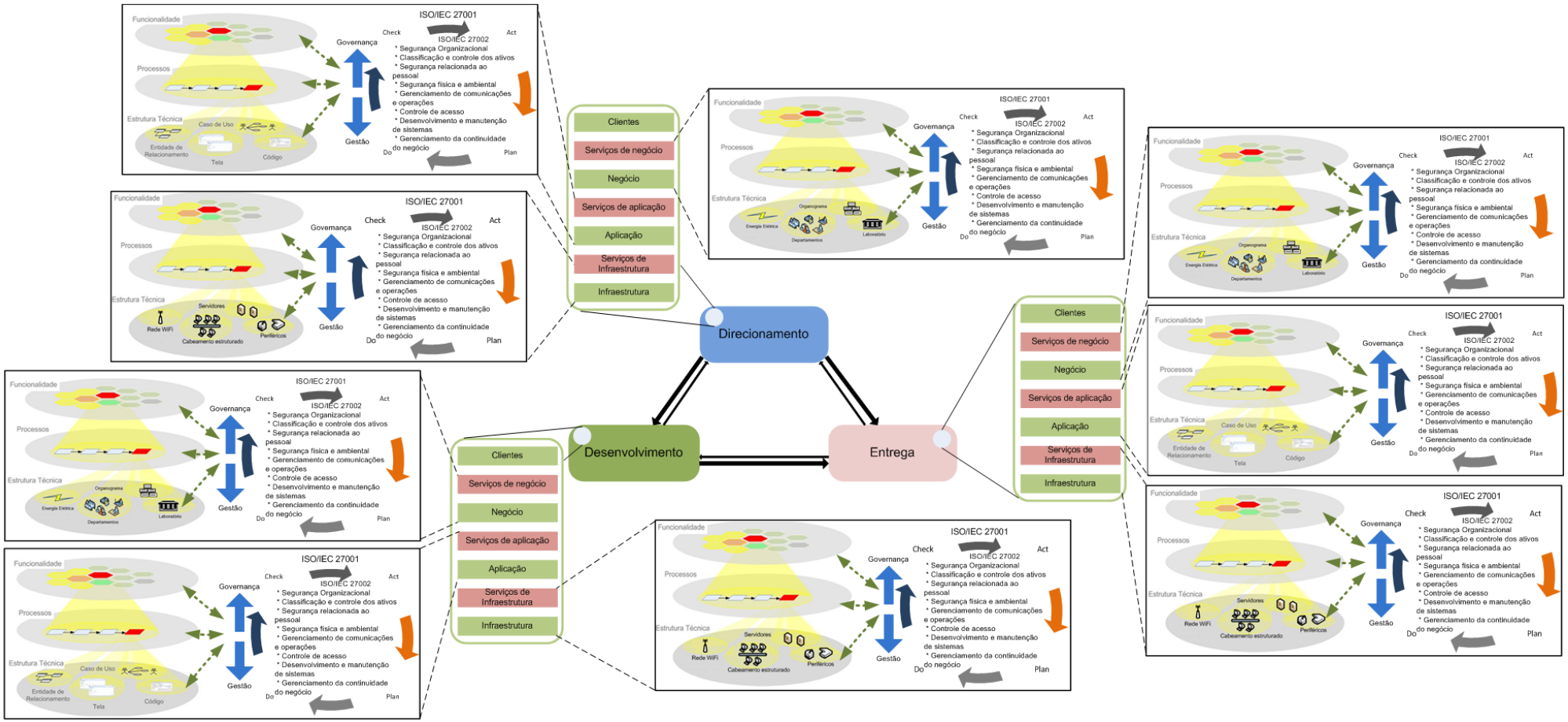


Figura 3.5 - Integração entre os modelos propostos – Visão completa

A governança de TI busca compartilhar decisões de TI com os demais dirigentes da organização, assim como estabelece regras à organização e aos processos que nortearão o uso da Tecnologia da Informação pelos usuários, departamentos, divisões, negócios da organização, fornecedores e clientes, determinando como a TI deve prover os serviços para a empresa**[**48**]**.

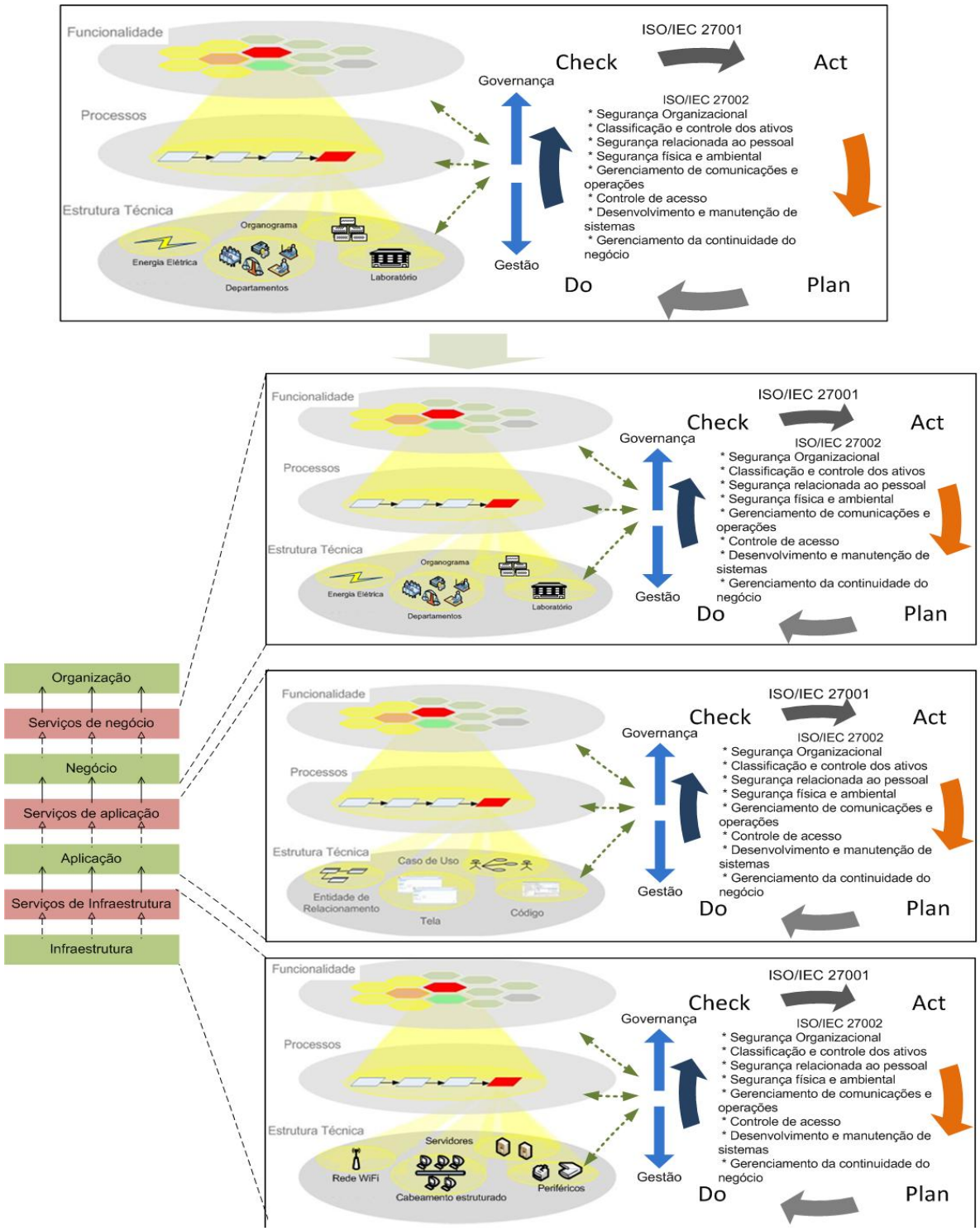


Figura 3.6 - Navegação pelas informações
Fonte: [**49**], com adaptações.

A necessidade de corresponder às expectativas dos clientes aos objetivos organizacionais tornou o aprendizado parte do diferencial competitivo [**28**]. O conceito do modelo PDCA evoluiu ao longo dos anos vinculando-se também a idéia de que, uma organização qualquer, encarregada de atingir um determinado objetivo, necessita planejar e controlar as atividades a ela relacionadas. Aprender a aperfeiçoar os conceitos de melhoria contínua, as técnicas e práticas de gerenciamento de projetos e ainda construir um sistema de gestão voltado ao constante aprendizado elevou a consciência para a importância dos ativos intangíveis nas organizações [**28**].

Uma parte integrante da governança corporativa é a governança de TI, que consiste no gerenciamento das estruturas organizacionais e dos processos, a fim de assegurar a sustentabilidade e a ampliação da estratégia e dos objetivos da organização ITGI *apud* Grembergen. A figura 3.7 representa aspectos de governança e gerenciamento que envolve a avaliação dos resultados do negócio, definição da estratégia e o aprimoramento dos modelos de negócio, por meio do procedimento de tomada de decisão. O gerenciamento de TI centra-se na representação de ações definidas pela arquitetura corporativa desejada em sua estratégia concentrado seus esforços nos serviços/produtos internos de TI e na gestão eficiente e eficaz das operações presentes[**4**] [**50**] [**52**].

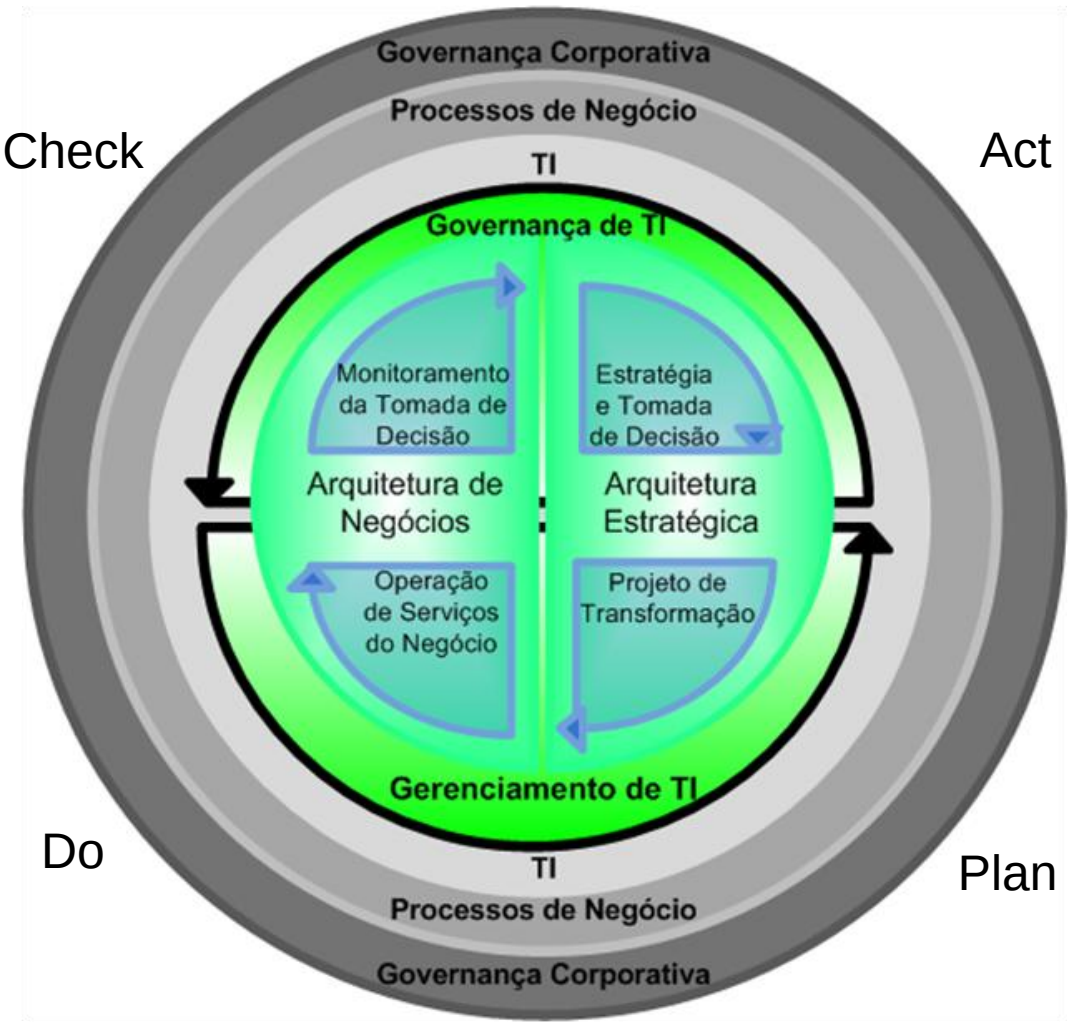


Figura 3.7 - Ciclo de governança e gestão corporativa de TI
Fonte: [**3**], com adaptações

Dessa forma a modelagem de uma organização deve estar pautada na transcrição da realidade e suas ações devem ser descritas em uma relação representada por uma cadeia de governança. Esta cadeia estabelece o processo de gestão com a execução de suas tarefas representadas na arquitetura corporativa atual (denominada arquitetura de negócios) bem como, o processo de governança que constitui a melhoria continua dos processos existentes estabelecendo uma relação transformacional descrita pela arquitetura organizacional desejada (denominada arquitetura estratégica), onde projetos definidos passam para a escala da operacionalização.

As normas ISO/IEC 27001 e ISO/IEC 27002 podem ser utilizadas considerando o ciclo de vida do PDCA tanto para atividades de governança quanto de gestão conforme demonstra a Figura 3.8.

Figura 3.8 - Governança e gestão integradas ao PDCA e as normas ISO/IEC 27001 e 27002

No cenário de transição descrito pela arquitetura corporativa atual (arquitetura de negócios) e arquitetura corporativa desejada (arquitetura estratégica) observa-se a possibilidade de aplicação do modelo PDCA como forma de exercer os controles e o processo de melhoria contínua da organização, de acordo com o que é demonstrado na Figura 3.9.

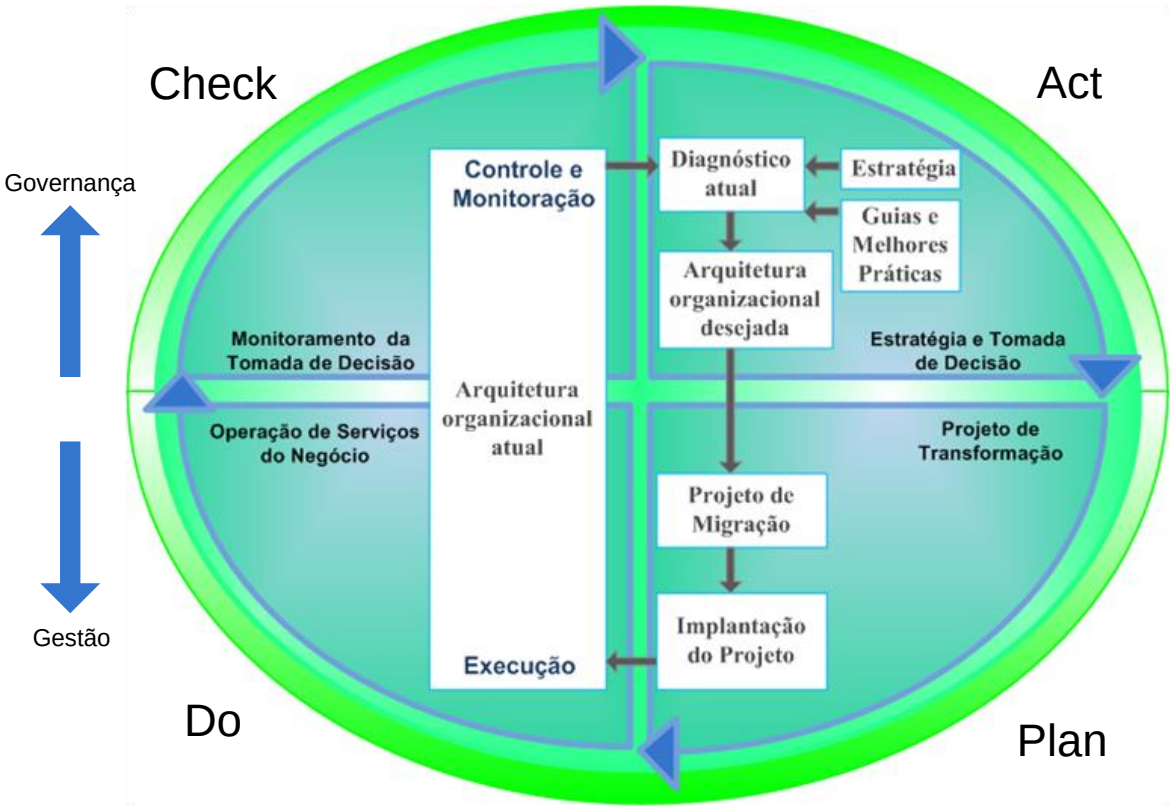


Figura 3.9 - Processo transformacional da cadeia de governança
Fonte: [**3**], com adaptações

De acordo com [**3**], o ciclo de governança e gestão (CGG) é dividido em etapas, como forma de operacionalização. Estas etapas visam o alinhamento organizacional e estão descritas na Tabela 3.1, que segue abaixo.

Tabela 3.1 - Etapas do Ciclo de governança e gestão

ETAPA	DESCRIÇÃO	PDCA
Etapa 1 – Estratégia	O contexto da organização é analisado a fim de se encontrar novas oportunidades, tendências ou uma adequação a determinada situação. Nesta fase é elaborado o planejamento estratégico e o gerenciamento da estratégia.	*Act*
Etapa 2 – Guias de coleções e melhores práticas	Essa etapa foi desenvolvida para auxiliar a etapa 1. Consideram-se os guias de melhores práticas, que neste caso, incluem as normas ISO/IEC 27001 e ISO/IEC 27002. Os guias contêm princípios, políticas, regulamentações, leis, normas, frameworks, modelos e métodos.	*Act*

Etapa 3 – Arquitetura corporativa atual (controle e monitoramento)	Por meio da analise desta etapa concentra-se na avaliação do funcionamento da arquitetura corporativa atual. O monitoramento inclui a analise de indicadores de desempenho, processos, pessoas e tecnologia.	*Check*
Etapa 4 – Diagnóstico	Esta etapa define quais são as lacunas da arquitetura corporativa. Para tanto utiliza a estratégia, os guias e melhores práticas e a avaliação da arquitetura corporativa atual desenvolvidas nas etapas anteriores.	*Act*
Etapa 5 – Arquitetura corporativa desejada	Esta etapa é responsável por preencher as possíveis lacunas existentes identificados na etapa 4 por meio do desenvolvimento da proposta de melhoria que define a arquitetura corporativa desejada.	*Act*
Etapa 6 – Projeto de migração	Nesta etapa são definidas a equipe do projeto e os aspectos da gestão de mudança.	*Plan*
Etapa 7 – Implantação do projeto	Execução das etapas anteriores. Sugere-se a elaboração de um protótipo antes da implementação do produto na organização.	*Plan*
Etapa 8 – Arquitetura corporativa atual (execução)	Operação da nova arquitetura corporativa.	Do

Fonte: [**3**], pág. 193 e 194, com adaptações

A necessidade de corresponder às expectativas dos clientes aos objetivos organizacionais tornou o aprendizado uma forma de diferencial competitivo. Aprender a aperfeiçoar conceitos de melhoria contínua, com as técnicas e práticas de gerenciamento de projetos e ainda construir um sistema de gestão voltado para o constante aprendizado, elevou a consciência dos líderes da organização para a importância dos ativos intangíveis nas organizações. O interesse das organizações no conhecimento advém da necessidade de superar desafios, diferenciando-se pelo que sabem e pela forma como conseguem usar esse conhecimento [**33**].

4 APLICAÇÃO DE UM ESTUDO DE CASO COM VISTAS A INTEGRAÇÃO DA SEGURANÇA À GESTÃO DE TI

O propósito deste trabalho é prover uma visão diferenciada de análise de uma organização com intuito de integrar a segurança à gestão de TI e, para tanto, utiliza o modelo de arquitetura de TI agregada à visão do modelo sistêmico dos trios por meio das normas ISO/IEC 27001 e ISO/IEC 27002.

Os seguintes aspectos devem ser considerados:

- A aplicação conjunta dos conceitos relativos ao ciclo de governança e gestão alinhado ao PDCA, acerca dos domínios de TI: Negócio, Aplicação e Infraestrutura para cada subsistema de TI;
- Delinear a partir da aplicação conjunta dos conceitos relativos ao CGG alinhado ao PDCA a análise sistêmica dos conceitos: *i)* Funcionalidade; *ii)* Processo e, *iii)* Estrutura, como fatores a serem considerados à efetivação da segurança da informação no ambiente do estudo de caso, bem como o estabelecimento de um processo de gestão da Segurança da Informação.
- Aplicar os controles necessários, com base nas normas ISO/IEC 27001 e ISO IEC 27002, aos subsistemas de TI preservando sua especificidade e considerando suas funcionalidades descritas no processo de analise descrito nos tópicos anteriores.

Considerando que a gestão da segurança é um conjunto de regras e práticas que regulam como uma organização gerencia, cria, e distribui suas informações de forma segura [**3**], a analise dos cenários envolvidos foi feita a partir da leitura dos conceitos de segurança da informação e seus relacionamentos descritos na Figura 4.1.

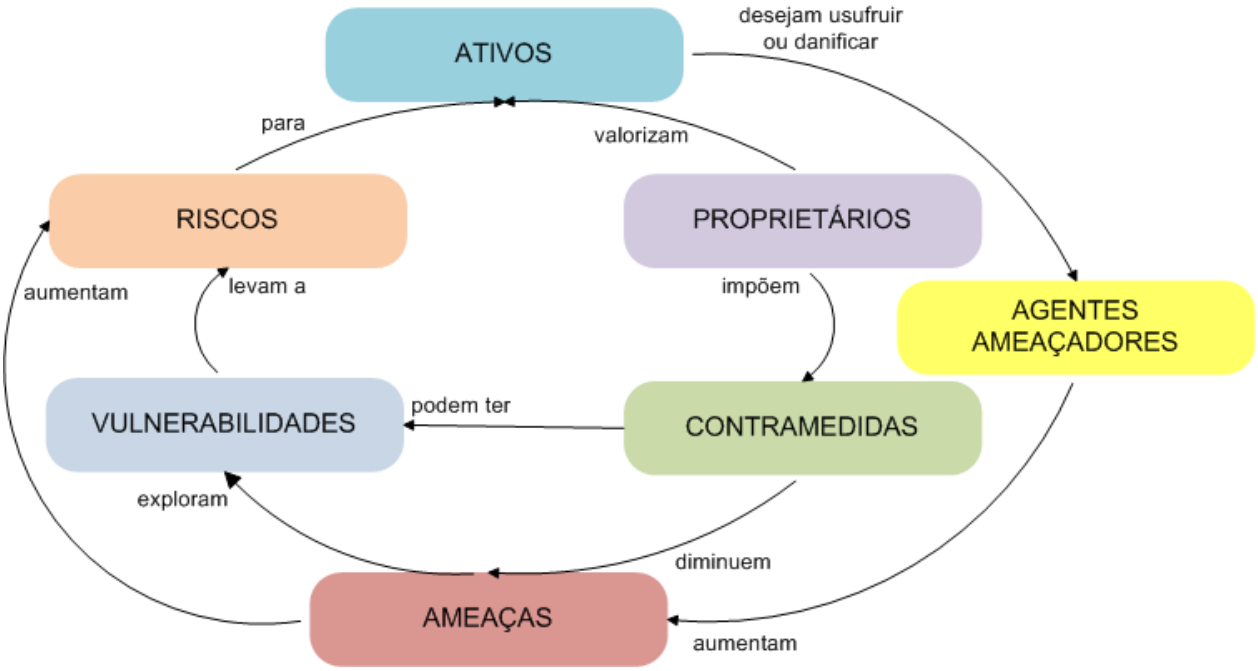


Figura 4.1 - Conceitos de segurança e seus relacionamentos
Fonte: [**3**]

A tabela 4.1 descreve a organização da informação adquirida no processo de governança e gerenciamento do ponto de vista de cada subsistema de TI (Direcionamento, Desenvolvimento e Entrega) alinhado as etapas do ciclo de governança, gestão e as fases do PCDA, executadas no domínio do Negócio, Aplicação e Infraestrutura no ambiente onde foi desenvolvido o estudo de caso. Nos domínios do Negócio, Aplicação e Infraestrutura foram integrados conceitos sistêmicos do trio (Funcionalidade, Processos e Estrutura).

Tabela 4.1 - Estrutura de alinhamento entre modelos

SUBISTEMA DE TI (DIRECIONAMENTO / DESENVOLVIMENTO / ENTREGA)		
CICLO DE GOVERNANÇA E GESTÃO ALINHADO COM O PDCA	NEGÓCIO	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA
	APLICAÇÃO	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA
	INFRAESTRUTURA	FUNCIONALIDADE
		PROCESSO
		ESTRUTURA

4.1 CONTEXTUALIZAÇÃO DO CENÁRIO

A produção de conhecimento na UnB está pautada no trio: ensino, pesquisa e extensão; para favorecer a formação universitária de qualidade. Para dar apoio às atividades desenvolvidas na UnB, alunos, professores e servidores contam com 400 laboratórios, além dos órgãos de apoio, como o Hospital Universitário e a Biblioteca Central [**53**].

O presente estudo de caso foi realizado em um laboratório, pertencente à Universidade de Brasília, voltado à pesquisa, desenvolvimento e a aplicação de novas tecnologias no campo da educação, das telecomunicações e das tecnologias da informação. O laboratório é dotado de uma moderna infraestrutura tecnológica, educacional e organizacional e se dedica ao desenvolvimento e aplicação de tecnologias avançadas em telecomunicações e informática.

O laboratório está dividido em duas unidades localizadas em pontos diferentes dentro do campus universitário. As unidades são compostas por estruturas físicas semelhantes, com relação à equipamentos, mobiliário e estúdios para vídeo conferência, produção visual e ambiente virtual que constituem parte dos ativos da unidade acadêmica. As unidades são logicamente interligadas por meio de uma rede de computadores dotados de acesso à internet.

O acesso aos ambientes físicos é feito por meio de um sistema de chaveamento de controle de acesso digital com a utilização de senha única e somente pessoas autorizadas possuem acesso. A segurança física desses ambientes dispõe do emprego deste controle de acesso digital e, também, utiliza um controle manual (fechadura).

Os usuários da rede de comunicação interna são cadastrados em um domínio comum, caracterizando o perfil de rede do laboratório. Com esse perfil os usuários podem acessar aos sistemas, *softwares* e documentos pertencentes ao laboratório e as pesquisas realizadas. Toda a produção e pesquisa científica do laboratório, que é caracterizada como ativo, é armazenada em um servidor de dados. Informações particulares dos usuários armazenadas no servidor não são de responsabilidade do laboratório.

O perfil de usuário do laboratório está dividido de acordo com a área de atuação do colaborador que pode ser: acadêmico, produção, secretaria (administrativa) e TI. Assim, cada usuário possui acesso apenas aos dados referentes à sua área de atuação, ficando os colaboradores da TI com privilégios administrativos para controle e manutenção de todas as informações armazenadas.

O *backup* das informações do servidor de dados é feito por meio de cópia das informações em unidades externas utilizando um algoritmo de rotina de cópia de arquivo. O processo de *backup* se dá por meio de agendamento prévio de dia e horário respeitando os seguintes critérios: realizar o *backup* pelo menos uma vez por semana e utilizar a rede no horário de menor demanda para evitar o trafego desnecessário e não comprometer as atividades do laboratório.

Vale ressaltar que o setor de TI é responsável por estabelecer a estrutura de *backup* e sua manutenção. Os dados que serão copiados são de responsabilidade de cada colaborador que por sua vez armazena a informação em pastas devidamente identificadas e com tratamento da segurança para acesso da informação estabelecido. Somente o colaborador que possui permissão para acessar determinada pasta tem privilégio administrativo sobre os arquivos armazenados, bem como para acessá-los ou modificá-los.

A estrutura da segurança lógica da informação é feita por meio de *firewall* e antivírus. A manutenção da rede de computadores é empreendida por colaboradores especializados, assim, rotinas de controle de entrada de *softwares* maliciosos são feitas com regularidade, da mesma forma como há rotina de *backup* estabelecida.

O laboratório, então, é freqüentado por professores, pesquisadores, demais colaboradores como alunos de graduação e pós-graduação que possuem uma relação direta com o núcleo de estudos e pesquisa. Para estes, é informado a senha numérica de acesso físico aos ambientes.

4.1.1 Acesso de pessoas não autorizadas ao ambiente físico dos laboratórios

Conforme foi descrito, o acesso físico aos laboratórios é feito por meio de uma autenticação numérica (senha) única em um equipamento de chaveamento digital e por um sistema de controle manual. Assim, o primeiro colaborador a chegar ao laboratório, no

inicio do expediente, destrava o controle manual com a utilização da chave e os demais colaboradores realizam a entrada utilizando somente o chaveamento digital e este processo se repete ao longo do dia. Ao final do expediente, o ultimo colaborador a sair do laboratório se responsabiliza por trancá-lo com a utilização da chave.

Monitorando-se o acesso, foi possível observar que o laboratório também era frequentado por pessoas não integrantes do laboratório. Em função da diversidade de informações, equipamentos e *softwares* disponíveis nos ambientes, a segurança passou a ser questionada. A utilização de uma senha única para abertura da porta tornou-se ineficiente diante do não sigilo do seu valor.

Realizando uma leitura da problemática observada baseada nos conceitos de segurança, tem-se que o não sigilo da senha de acesso físico ao ambiente descreve uma vulnerabilidade aos ativos caracterizando riscos associados e possíveis ameaças. A necessidade do estabelecimento de contramedidas foram registradas e informadas aos tomadores de decisão (*stakeholders)* do laboratório e, desta forma, foi empreendida uma analise critica da atual política de segurança a ser avaliada.

A direção do laboratório verificou a necessidade de modificação do processo atual considerando que os controles descritos pela norma ISO/IEC 27002, especificamente, seção 7 – Segurança física e ambiental, objetivo de controle 7.1 – áreas de segurança e controle 7.1.2 – controle para entrada física que descreve que as áreas de segurança devem ser protegidas por controles de entrada apropriados, para garantir apenas o pessoal autorizado tenha acesso a elas [**42**].

O setor do Desenvolvimento recebeu as orientações descritas pelo Direcionamento e passou a ser responsável pelo incremento dos projetos aprovados. Assim, suportou a construção de soluções baseadas nos projetos autorizados com as diretrizes de governança determinadas pelo Direcionamento.

Diante do contexto, observou-se que o controle de acesso digital com a utilização de senha única não estava atendendo. A primeira solução construída pelo setor de Entrega foi a realização da troca periódica das senhas únicas de acesso. A nova senha foi redistribuída aos colaboradores que frequentam os laboratórios.

Decorrido certo tempo, em um processo de avaliação interna do laboratório, analisou-se que a problemática anterior se repetia e, igualmente, a necessidade de reestruturação do controle de acesso físico era necessária. Pensando no processo de melhoria contínua dos processos, a direção do laboratório verificou novamente a necessidade de modificação do processo atual considerando que os mesmos controles descritos pela norma ISO/IEC 27002 (seção 7 – Segurança física e ambiental, objetivo de controle 7.1 – áreas de segurança e controle 7.1.2 – controle para entrada física) estavam fragilizados diante da exposição do valor numérico da senha de controle ao acesso físico.

O setor do Desenvolvimento recebeu as novas orientações descritas pelo Direcionamento, que sugeriu uma possível troca de tecnologia e passou a ser responsável pelo incremento dos projetos aprovados. A construção da solução baseada nos projetos determinadas pelo Direcionamento de tal forma que o setor de Entrega, responsável pela operação das atividades e pelas soluções desenvolvidas, realizou a troca do equipamento, com uma senha de acesso físico individualiza e personificada por meio da leitura biométrica (digital).

Para a troca do equipamento não foram necessárias mudanças na estrutura física dos laboratórios uma vez que o novo sistema não está ligado ao sistema de rede. Cada equipamento instalado possui memória suficiente para armazenar a quantidade de usuários que frequentam o laboratório.

Com a utilização do padrão de senha individual para os colaboradores dos laboratórios a fragilidade decorrente do acesso indevido de entrada física foi mitigada e os controles descritos pela norma ISO/IEC 27002 (seção 7 – Segurança física e ambiental, objetivo de controle 7.1 – áreas de segurança e controle 7.1.2 – controle para entrada física) foram alinhados ao processo de gestão da segurança.

A aplicação do ciclo de governança e gestão com foco na melhora dos controles descritos pela norma ISO/IEC 27002 (seção 7 – Segurança física e ambiental, objetivo de controle 7.1 – áreas de segurança e controle 7.1.2 – controle para entrada física) está concatenada por subsistema de TI e pelas etapas do CGG.

4.1.2 Subsistema de TI: Direcionamento

O subsistema de TI, Direcionamento, dentro do escopo da etapa 1 do CGG (estratégia) é descrito pela Tabela 4.2. Sob o ponto de vista do domínio, Negócio, é necessário a melhoria do serviço de controle de acesso. Nesse quesito, a Funcionalidade do controle de acesso se preserva e não precisa sofrer alterações, no entanto, o Processo para controle de acesso físico necessitará de alterações do teclado de digitação manual, com senha única, para um leitor biométrico, com senha individual.

Nos domínios Aplicação e Infraestrutura não há necessidade de alteração, pois o atributo desejado não provoca mudanças nesses domínios; e, respectivamente, a Funcionalidade, Processos e Estrutura não sofreram alterações.

Tabela 4.2 - Etapa 1 – Estratégia no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Direcionamento

SUBSISTEMA DE TI: DIRECIONAMENTO				
ETAPA 1 - ESTRATÉGIA (*ACT*)	NEGÓCIO	Melhorar os serviços de controle de acesso	FUNCIONALIDADE	A mesma funcionalidade
			PROCESSO	Verificar a necessidade de modificação do processo - atual: senha comum; desejado: senha individual.
			ESTRUTURA	Verificar a necessidade de modificação de equipamento - atual: teclado numérico; desejado: leitor biométrico.
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRA ESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A Tabela 4.3 apresenta no subsistema de TI Direcionamento a etapa 2 do ciclo de governança e gestão (Guias e coleções de melhores práticas) onde o domínio Negócio, fundamentado pela Norma ISO/IEC 27002, ressalta a necessidade de melhorar a seção 7 – segurança física e ambiental, o controle 7.1.2 – controle para entrada física cujo o objetivo de controle 7.1 – áreas de segurança e controle. Considerando a modificação do Processo atual para um processo que tenha aderência a norma e a verificação da necessidade de alteração do equipamento sob o ponto de vista da Estrutura com o foco na observância da

norma. Ressalta-se ainda que nos domínios Aplicação e Infraestrutura não há necessidade de alteração, pois a aderência desejada não provoca mudanças nesses domínios e, respectivamente, a Funcionalidade, Processos e Estrutura não sofrem alterações.

Tabela 4.3 - Etapa 2 – Guias e coleções de melhores práticas no processo e governança e gestão da segurança nos laboratórios – Subsistema de TI Direcionamento

SUBSISTEMA DE TI: DIRECIONAMENTO				
ETAPA 2 - GUIAS E COLEÇÕES DE MELHORES PRÁTICAS (*ACT*)	NEGÓCIO	Melhorar a seção 7 -Segurança Física e Ambiental - ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade com foco na seção 7 - ISO/IEC 27002
			PROCESSO	Modificação do processo atual com foco na seção 7 - ISO/IEC 27002
			ESTRUTURA	Verificar a necessidade de modificação de equipamento com foco na seção 7 - ISO/IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A etapa 3 (arquitetura atual) se concentra em avaliar o funcionamento da arquitetura corporativa atual, onde seu monitoramento inclui a analise de indicadores de desempenho, processos, pessoas e tecnologia. A etapa 4 (diagnóstico) define quais são as lacunas da arquitetura corporativa.

Conforme tabela 4.4, a aplicação do CGG nestas etapas e com o foco no subsistema de TI, Direcionamento, descreve o atendimento ineficaz da seção 7 – segurança física e ambiental o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física descrito na Norma ISO/IEC 27002 tanto para o Negócio quanto para a Aplicação.

Assim, no domínio, Negócio, sugere a manutenção do atendimento da Funcionalidade que é a continuidade de controle de acesso físico, porém com acolhimento normativo. Para Processos, a proposta é a modificação do processo atual (controle de

acesso físico com a utilização de senha única) e para Estrutura a sugestão é verificar a necessidade de modificação de equipamento em atendimento a norma citada.

Nos itens, Aplicação e Infraestrutura, para os conceitos sistêmicos de Funcionalidade, Processos e Estrutura não sofrem alteração, pois nesta etapa se considera a estrutura e a analise de diagnostico da situação corporativa atual.

Tabela 4.4 – Etapas 3 e 4 – Arquitetura atual (controle e monitoramento) e diagnóstico no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Direcionamento

SUBSISTEMA DE TI: DIRECIONAMENTO				
ETAPA 3 e 4 - ARQUITETURA ATUAL (CONTROLE,MONITORAMENTO) E DIAGNÓSTICO (*CHECK* e *ACT*)	NEGÓCIO	Através do monitoramento da arquitetura atual, verifica-se o atendimento ineficaz da seção 7, objetivo de controle 7.1, controle 7.1.2 ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade com foco na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Modificação do processo atual com foco na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Verificar a necessidade de modificação de equipamento com foco na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A tabela 4.5 apresenta a arquitetura corporativa desejada onde o domínio, Negócio, no subsistema de TI, Direcionamento, descreve que a arquitetura corporativa deve atender de forma efetiva os controles descritos pela Norma ISO/IEC 27002 (seção 7 –

segurança física e ambiental o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física), ou seja, o controle de acesso físico deve ser eficaz e eficiente ao que se destina fazer e os conceitos sistêmicos visam:

- Funcionalidade: manter a funcionalidade de controle de acesso físico, entretanto com indicação de maior efetividade do controle de acesso físico atual e em conformidade com as normas apresentadas;
- Processo: alinhar os processos de negócio com base na aplicação da norma a fim de individualizar o controle de acesso físico aos ambientes do laboratório;
- Estrutura: modificar o equipamento de controle de acesso físico atual de forma a atender aos requisitos anteriormente descritos. Considerar que as etapas anteriores do CGG descritas dão suporte para o entendimento da necessidade exigida para um novo equipamento.

Os domínios Aplicação e Infraestrutura tanto em sua definição, quanto nos conceitos sistêmicos, Funcionalidade, Processo e Estrutura, não são alterados, pois a nova tecnologia adotada não utilizará nenhum recurso com a modificação da aplicação ou da infraestrutura existente.

Tabela 4.5 - Etapa 5 – Arquitetura corporativa desejada no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Direcionamento

SUBSISTEMA DE TI: DIRECIONAMENTO				
ETAPA 5 - ARQUITETURA CORPORATIVA DESEJADA (*ACT*)	NEGÓCIO	A arquitetura corporativa desejada deve atender efetivamente a seção 7, objetivo de controle 7.1, controle 7.1.2 ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade com maior efetividade com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Alinhamento do processo desejado com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Modificar o equipamento de controle de acesso físico com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002

	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A etapa 6 do CGG descreve a definição da equipe do projeto e os aspectos da gestão de mudança. Desse modo, a Tabela 4.6, refere-se ao subsistema de TI Direcionamento, no domínio do Negócio propondo testes com base na Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física.

Os referidos testes devem considerar conceitos sistêmicos: *i)* Funcionalidade – verificar a efetividade da mesma funcionalidade atual, ou seja, conferir se a operacionalidade do controle de acesso físico está preservada; *ii)* Processo – testar o alinhamento dos processos propostos estão em conformidade normativa, e por fim, *iii)*Estrutura – testar se a modificação do equipamento de controle de acesso físico está observando as normas existentes.

Para os domínios Aplicação e Infraestrutura os conceitos sistêmicos Funcionalidade, Processo e Estrutura não sofrem alteração, pois não foram detectadas mudanças para esses componentes.

Tabela 4.6 – Etapa 6 – Projeto de migração no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Direcionamento

SUBSISTEMA DE TI: DIRECIONAMENTO				
ETAPA 6 - PROJETO DE MIGRAÇÃO (*PLAN*)	NEGÓCIO	A arquitetura corporativa desejada deve ser testada conforme seção 7, objetivo de controle 7.1, controle 7.1.2 ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade deve ser testada para verificar a sua efetividade com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002

			PROCESSO	Alinhamento do processo desejado deve ser testado com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	A Modificação do equipamento de controle de acesso físico deve ser testado com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A etapa 7 descreve a governança da execução das etapas anteriores. Assim a Tabela 4.7, no ponto de vista do subsistema de TI Direcionamento, delineia no domínio Negócio sobre a implantação da arquitetura corporativa desejada com apoio na Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física. Dessa maneira, os conceitos sistêmicos do trio definem:

- Funcionalidade :implantar a mesma funcionalidade referente ao controle de acesso físico de forma a verificar se o novo sistema atende em efetividade e possui aderência as normas relacionadas;
- Processo: implantar o alinhamento dos processos descrito pelas etapas anteriores do CGG;
- Estrutura: Implantar a modificação do equipamento de controle de acesso físico.

Os domínios Aplicação e Infraestrutura, bem como o conceito sistêmico do trio Funcionalidade, Processo e Estrutura, não suportam mudanças na etapa 7 pois a tecnologia descrita na arquitetura corporativa atual não afeta estes requisitos.

Tabela 4.7 – Etapa 7 – Implantação do projeto no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Direcionamento

SUBSISTEMA DE TI: DIRECIONAMENTO				
ETAPA 7 - IMPLANTAÇÃO DO PROJETO (*PLAN*)	NEGÓCIO	A arquitetura corporativa desejada deve ser implantada conforme seção 7, objetivo de controle 7.1, controle 7.1.2 ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade deve ser implantada para verificar a sua efetividade com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Alinhamento do processo desejado deve ser implantada com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	A Modificação do equipamento de controle de acesso físico deve ser implantado com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A etapa 8 descreve a operação da nova arquitetura corporativa sob o ponto de vista do subsistema de TI Direcionamento. Para o domínio Negócio descreve-se a execução da arquitetura corporativa desejada conforme a Norma ISO/IEC 27002, seção 7 –

segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física.

A Funcionalidade neste domínio demonstra a execução da mesma funcionalidade de controle de acesso físico em conformidade com a norma. O conceito sistêmico, Processo, refere-se à efetivação das ações de alinhamento da arquitetura corporativa desejada e a Estrutura propõe a execução da modificação do equipamento de controle de acesso físico respeitando as normas destacadas.

Para os domínios Aplicação e Infraestrutura os conceitos sistêmicos Funcionalidade, Processo e Estrutura não sofrem alteração, pois não foram provisionados execuções para esses elementos.

Tabela 4.8 – Etapa 8 – Arquitetura corporativa atual do projeto no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Direcionamento

SUBSISTEMA DE TI: DIRECIONAMENTO				
ETAPA 8 - ARQUITETURA CORPORATIVA ATUAL (EXECUÇÃO) (DO)	NEGÓCIO	A arquitetura corporativa desejada em produção conforme seção 7, objetivo de controle 7.1, controle 7.1.2 ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade em produção com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Alinhamento do processo desejado em produção com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	A Modificação do equipamento de controle de acesso físico em produção com base na seção 7, objetivo de controle 7.1, controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

Alinhamento com PDCA com o CGG para o subsistema de TI Direcionamento

O subciclo de governança envolve o processo de tomada de decisão e no CGG e engloba as fases de *Check* e *Act* do PDCA. As atividades referentes ao alinhamento podem ser descritas como:

- Governança: *Check*: Para a Norma ISO/IEC 27001 o *Check* corresponde a atividade de avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do sistema de gestão da segurança da informação (SGSI) e apresentar os resultados para a análise crítica pela direção.

Resultado principal da fase *Check* no direcionamento – verifica-se que o serviço de controle de acesso físico existente não tem impedido a entrada de pessoas não autorizadas.

- Governança – *Act*: Para a Norma ISO/IEC 27001 o *Act* corresponde a execução de ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Resultado principal da fase *Act* no direcionamento – decide-se pela aprovação de um projeto de melhoria do serviço de controle de acesso físico existente, pois não tem impedido a entrada de pessoas não autorizadas.

O subciclo de gestão envolve o acompanhamento das atividades de execução do processo de tomada de decisão anterior e no CGG engloba as fases de *Plan* e *Do* do PDCA.As atividades referentes ao alinhamento podem ser descritas:

- Gestão – *Plan*: Para a Norma ISO/IEC 27001 o *Plan* estabelece a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de

riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

Resultado principal da fase *Plan* no direcionamento – Informar e acompanhar o projeto de melhoria do serviço de controle de acesso físico existente de forma a atender integralmente Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física e mitigar a entrada de pessoas não autorizadas no âmbito do laboratório.

- Gestão – *Do*: Para a Norma ISO/IEC 27001 a fase *do* implementa e opera a política, controles, processos e procedimentos do SGSI.

Resultado principal da fase *Do* no direcionamento – acompanhar a implantação do projeto de melhoria do serviço de controle de acesso físico existente, no subsistema de TI Desenvolvimento e a sua implantação no subsistema de TI Entrega.

O alinhamento entre o subciclo governança, que abrange o processo de tomada de decisão descrito pelas fases *Check* e *Act* do PDCA; com o subciclo gestão, que envolve o acompanhamento das atividades de execução do processo de tomada de decisão anterior e no CGG engloba as fases de *Plan* e *Do* do PDCA, inseridos no subsistema de TI Direcionamento onde sua principal funcionalidade é o planejamento e o controle de alto nível, está representado pela Figura 4.2.

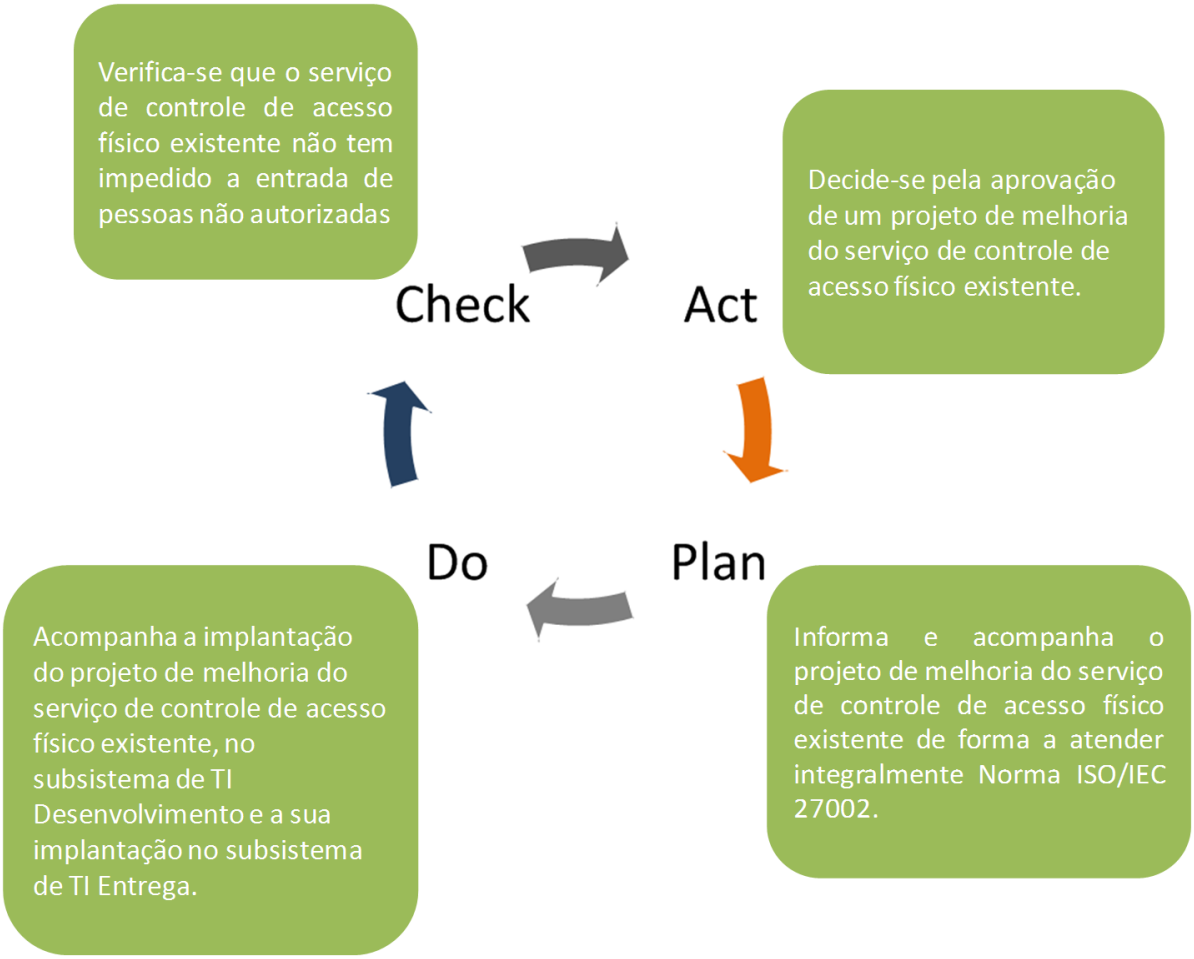


Figura 4.2 - Alinhamento com PDCA com o CGG para o subsistema de TI Direcionamento

4.1.3 Subsistema de TI: Desenvolvimento

O subsistema, Desenvolvimento, possui como funcionalidade essencial a construção de soluções e o incremento de suas atividades baseada nos projetos autorizados e com as diretrizes de governança determinadas pelo Direcionamento.

A tabela 4.9 descreve, no subsistema de TI, Desenvolvimento, a etapa 1 do CGG (estratégia). Sob o ponto de vista do domínio, Negócio, identifica-se a necessidade de projetar as modificações na arquitetura atual para melhorar o serviço de controle de acesso físico de tal forma a preservar a Funcionalidade, considerando a sugestão de modificação do Processo (utilização de senha única comum para senha individualizada) e a sugestão de modificação da Estrutura descrita pela alteração do equipamento atual (equipamento com teclado numérico para equipamento com leitor biométrico).

Nos domínios Aplicação e Infraestrutura não há necessidade de alteração, pois o atributo desejado não provoca mudanças nesses domínios e, respectivamente, a Funcionalidade, Processos e Estrutura não sofreram alterações.

Tabela 4.9 – Etapa 1 – Estratégia no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Desenvolvimento

SUBSISTEMA DE TI: DESENVOLVIMENTO				
ETAPA 1 - ESTRATÉGIA	NEGÓCIO	Projetar as modificações na arquitetura atual para melhorar o serviço de controle de acesso	FUNCIONALIDADE	A mesma funcionalidade
			PROCESSO	Sugestão de Modificação do processo aceita- atual: senha comum; desejado: senha individual
			ESTRUTURA	Sugestão de modificação do equipamento acatada- atual: teclado numérico; desejado: leitor biométrico
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A etapa 2 do CGG (Guias e coleções de melhores práticas) incorporado no subsistema de TI Desenvolvimento representado Tabela 4.10, descrito pelo domínio, Negócio, e fundamentado pela Norma ISO/IEC 27002, ressalta a necessidade de projetar sua melhora com base na seção 7 – segurança física e ambiental, o controle 7.1.2 – controle para entrada física cujo o objetivo de controle 7.1 – áreas de segurança e controle.

Para tanto, considera-se a mesma Funcionalidade já existente, a aprovação do seu Processo de modificação e da alteração na Estrutura por meio do equipamento de controle de acesso físico aderente as normas estabelecidas. Ressalta-se, ainda, que nos domínios Aplicação e Infraestrutura não há necessidade de alteração, pois a aderência desejada não provoca mudanças nesses domínios e, respectivamente, a Funcionalidade, Processos e Estrutura não sofrem modificação.

Tabela 4.10 – Etapa 2 – Guias e coleções de melhores práticas no processo e governança e gestão da segurança nos laboratórios – Subsistema de TI Desenvolvimento

SUBSISTEMA DE TI: DESENVOLVIMENTO				
ETAPA 2 - GUIAS E COLEÇÕES DE MELHORES PRÁTICAS	NEGÓCIO	Projetar a melhora com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade com foco na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			PROCESSO	Modificação do processo acatada com foco na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			ESTRUTURA	Modificação do equipamento acatada com foco na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

Conforme a tabela 4.11, é possível visualizar a aplicação do CGG nas etapas 3 e 4 (arquitetura atual e diagnóstico) foi empreendida com o foco no subsistema de TI, Desenvolvimento. No domínio, Negócio, o projeto de serviço de controle de acesso deve ser revisto de forma a atender a seção 7 – segurança física e ambiental,o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física descrito na Norma ISO/IEC 27002, de acordo com as decisões tomadas pelo subsistema Direcionamento.

Desta forma, o atendimento da Funcionalidade será mantido, porém com acolhimento normativo. Para Processos, descreve-se a modificação do processo atual (controle de acesso físico com a utilização de senha única) e para Estrutura, decidiu-se pela realização do projeto de modificação de equipamento em atendimento a norma citada.

Nos itens Aplicação e Infraestrutura para os conceitos sistêmicos de Funcionalidade, Processos e Estrutura não sofre alteração, pois nesta etapa se considera a estrutura e a analise de diagnostico da situação corporativa atual.

Tabela 4.11 – Etapas 3 e 4 – Arquitetura atual (controle e monitoramento) e diagnóstico no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Desenvolvimento

SUBSISTEMA DE TI: DESENVOLVIMENTO				
ETAPA 3 e 4 - ARQUITETURA ATUAL (CONTROLE, MONITORAMENTO) E DIAGNÓSTICO	NEGÓCIO	Por decisão do Direcionamento, o projeto de serviço de controle de acesso deve ser revisto em observância a seção 7, objetivo de controle 7.1, controle 7.1.2 ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade com foco na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			PROCESSO	Projetar modificação do processo com foco na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			ESTRUTURA	Projetar modificação do equipamento com foco na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A tabela 4.12 apresenta a arquitetura corporativa desejada onde o domínio Negócio no subsistema de TI, Desenvolvimento, descreve o projeto de serviço de controle de acesso revisto e modificado de maneira a atender efetivamente os controles descritos pela Norma ISO/IEC 27002 (seção 7 – segurança física e ambiental o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física) definidos pelo subsistema de TI, Direcionamento. Na prática, o controle de acesso físico deve ser eficaz e eficiente e os conceitos sistêmicos visam:

- Funcionalidade – manter a funcionalidade de controle de acesso físico, entretanto com indicação de maior efetividade para que o controle de acesso físico atual esteja em conformidade com a norma apresentada;
- Processo – projeção do alinhamento dos processos de negócio com base na aplicação da norma a fim de individualizar o controle de acesso físico aos ambientes do laboratório;

- Estrutura – introduzir as modificações necessárias aos equipamentos de controle de acesso físico atual de forma a atender aos requisitos anteriormente descritos.

Os domínios, Aplicação e Infraestrutura, tanto em sua definição, quanto nos conceitos sistêmicos, Funcionalidade, Processo e Estrutura, não serão alterados, pois a nova tecnologia adotada não utilizará nenhum recurso no qual sugira a realização de projeto de modificação da infraestrutura existente.

Tabela 4.12 – Etapa 5 – Arquitetura corporativa desejada no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Desenvolvimento

SUBSISTEMA DE TI: DESENVOLVIMENTO				
ETAPA 5 - ARQUITETURA CORPORATIVA DESEJADA	NEGÓCIO	Por decisão do Direcionamento, o projeto de serviço de controle de acesso foi revisto e modificado em observância a seção 7, objetivo de controle 7.1, controle 7.1.2 ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade com maior efetividade com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			PROCESSO	Projetar o alinhamento do processo desejado com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			ESTRUTURA	Introdução do novo equipamento de controle de acesso físico com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A Tabela 4.13 refere-se à etapa 6 do CGG para o subsistema de TI Desenvolvimento. No domínio, Negócio, são propostos testes necessários para o novo serviço de controle de acesso físico com base na Norma ISO/IEC 27002, seção 7 –

segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física.

Os referidos testes devem considerar conceitos sistêmicos: *i)* Funcionalidade – verificar a efetividade da mesma funcionalidade atual, ou seja, conferir se a operacionalidade do controle de acesso físico está preservada; *ii)* Processo – projetar os testes referentes ao alinhamento dos processos propostos estão em conformidade normativa e, por fim, *iii)* Estrutura – delinear a introdução do novo equipamento de controle de acesso físico em conformidade com as normas existentes.

Nos domínios, Aplicação e Infraestrutura, não foi identificada necessidade de elaboração de projeto de alterações. O mesmo vale para os conceitos sistêmicos, Funcionalidade, Processo e Estrutura, pois não foi provisionado mudanças para estes componentes.

Tabela 4.13 – Etapa 6 – Projeto de migração no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Desenvolvimento

SUBSISTEMA DE TI: DESENVOLVIMENTO				
ETAPA 6 - PROJETO DE MIGRAÇÃO	NEGÓCIO	O novo serviço de controle de acesso físico deve ser testado em observância a seção 7, objetivo de controle 7.1, controle 7.1.2 ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade deve ser testada para verificar a sua efetividade com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			PROCESSO	Projetar o alinhamento do processo desejado deve ser testado com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			ESTRUTURA	Introdução do novo equipamento de controle de acesso físico deve ser testado com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera

			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A etapa 7 do CGG é descrita pela Tabela 4.14, no ponto de vista do subsistema de TI Desenvolvimento, delineia no domínio Negócio sobre o processo de implantação do novo serviço de controle de acesso físico com apoio na Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física. Desta maneira, os conceitos sistêmicos do trio definem:

- Funcionalidade – executar a implantação da mesma funcionalidade referente ao controle de acesso físico de forma a verificar se o novo sistema atende em efetividade e possui aderência as normas relacionadas;
- Processo – executar o projeto de implantação do alinhamento dos processos descrito pelas etapas anteriores do CGG:
- Estrutura – introduzir o novo equipamento de controle de acesso físico com base no projeto de implantação da modificação do equipamento de controle de acesso físico.

Não se identifica a necessidade de implantação de projeto de alterações para os domínios, Aplicação e Infraestrutura. O mesmo vale para os conceitos sistêmicos, Funcionalidade, Processo e Estrutura, pois não foi provisionado mudanças para estes elementos.

Tabela 4.14 – Etapa 7 – Implantação do projeto no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Desenvolvimento

SUBSISTEMA DE TI: DESENVOLVIMENTO				
ETAPA 7 - IMPLANTAÇÃO DO PROJETO	NEGÓCIO	O novo serviço de controle de acesso físico deve ser implantado em observância a seção 7, objetivo de controle 7.1,	FUNCIONALIDADE	A mesma funcionalidade deve ser implantada com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002

		controle 7.1.2 ISO/IEC 27002	PROCESSO	Projetar o alinhamento do processo desejado deve ser implantado com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			ESTRUTURA	A introdução do novo equipamento de controle de acesso físico deve ser implantado com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A etapa 8 descreve a atividade da nova arquitetura corporativa sob o ponto de vista do subsistema de TI, Desenvolvimento, conforme Tabela 4.15. Para o domínio Negócio descreve-se o novo serviço de controle de acesso físico, conforme orientado pelo subsistema de TI Direcionamento e em observância a Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física.

A Funcionalidade neste domínio descreve a execução da mesma funcionalidade de controle de acesso físico em conformidade com a norma. O conceito sistêmico, Processo, refere-se à execução das ações de alinhamento da arquitetura corporativa desejada e a Estrutura propõe a execução da modificação do equipamento de controle de acesso físico respeitando as normas destacadas.

Nos domínios Aplicação e Infraestrutura não foram identificadas a execução de implantação de alterações para os conceitos sistêmicos Funcionalidade, Processo e Estrutura, pois não provisionado execuções para estes elementos.

Tabela 4.15 – Etapa 8 – Arquitetura corporativa atual do projeto no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Desenvolvimento

SUBSISTEMA DE TI: DESENVOLVIMENTO				
ETAPA 8 - ARQUITETURA CORPORATIVA ATUAL (EXECUÇÃO)	NEGÓCIO	O novo serviço de controle de acesso físico em produção em observância a seção 7, objetivo de controle 7.1, controle 7.1.2 ISO/IEC 27002	FUNCIONALIDADE	A mesma funcionalidade em produção com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			PROCESSO	O alinhamento do processo desejado em produção com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
			ESTRUTURA	A introdução do novo equipamento de controle de acesso físico em produção com base na seção 7, Objetivo de controle 7.1 e controle 7.1.2 - ISO /IEC 27002
	APLICAÇÃO	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

Alinhamento com PDCA com o CGG para o subsistema de TI Desenvolvimento

O subciclo de governança envolve o processo de tomada de decisão e no CGG engloba as fases de *Check* e *Act* do PDCA. As atividades referentes ao alinhamento podem ser descritas:

- Governança – *Check*: Para a Norma ISO/IEC 27001 o *Check* corresponde à atividade de avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do sistema de gestão da segurança da informação (SGSI) e apresentar os resultados para a análise crítica pela direção.

Resultado principal da fase *Check* no desenvolvimento – Revisão e análise do projeto de melhoria do serviço de controle de acesso físico existente em função da

identificação da problemática onde o sistema atual não tem impedido a entrada de pessoas não autorizadas e assim, fragilizando a gestão da segurança.

- Governança – *Act*: Para a Norma ISO/IEC 27001 o *Act* corresponde a execução de ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Resultado principal da fase *Act* no desenvolvimento – Desenvolver soluções com vista ao atendimento de diretrizes encaminhadas pelo subsistema de TI Direcionamento que estabelece a necessidade de revisão e avaliação do projeto de melhoria do serviço de controle de acesso físico existente, pois sistema atual de controle de acesso físico não tem impedido a entrada de pessoas não autorizadas e assim, fragilizando a gestão da segurança.

O subciclo de gestão envolve o acompanhamento das atividades de execução do processo de tomada de decisão anterior e no CGG engloba as fases de *Plan* e *Do* do PDCA. As atividades referentes ao alinhamento podem ser descritas:

- Gestão – *Plan*: Para a Norma ISO/IEC 27001 o *Plan* estabelece a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

Resultado principal da fase *Plan* no desenvolvimento – Proposição de solução tecnologia de forma a atender o projeto de melhoria do serviço de controle de acesso físico existente e em conformidade com a Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física e mitigar a entrada de pessoas não autorizadas no âmbito do laboratório.

- Gestão – Do: Para a Norma ISO/IEC 27001 o *do* implementa e opera a política, controles, processos e procedimentos do SGSI.

Resultado principal da fase *Do* no desenvolvimento – Desenvolvimento de um novo serviço de controle de acesso físico em atendimento as diretrizes instituídas pelo subsistema de TI Direcionamento e com aderência as normas estabelecidas.

O alinhamento entre o subciclo governança, que abrange o processo de tomada de decisão descrito pelas fases *Check* e *Act* do PDCA; com o subciclo gestão, que envolve o

acompanhamento das atividades de execução do processo de tomada de decisão anterior e no CGG engloba as fases de *Plan* e *Do* do PDCA, inseridos no subsistema de TI Desenvolvimento onde sua principal funcionalidade consiste em promover a construção de soluções e suas atividades estão pautadas nos projetos autorizados com as diretrizes de governança determinadas pelo Direcionamento, está representado pela Figura 4.3.

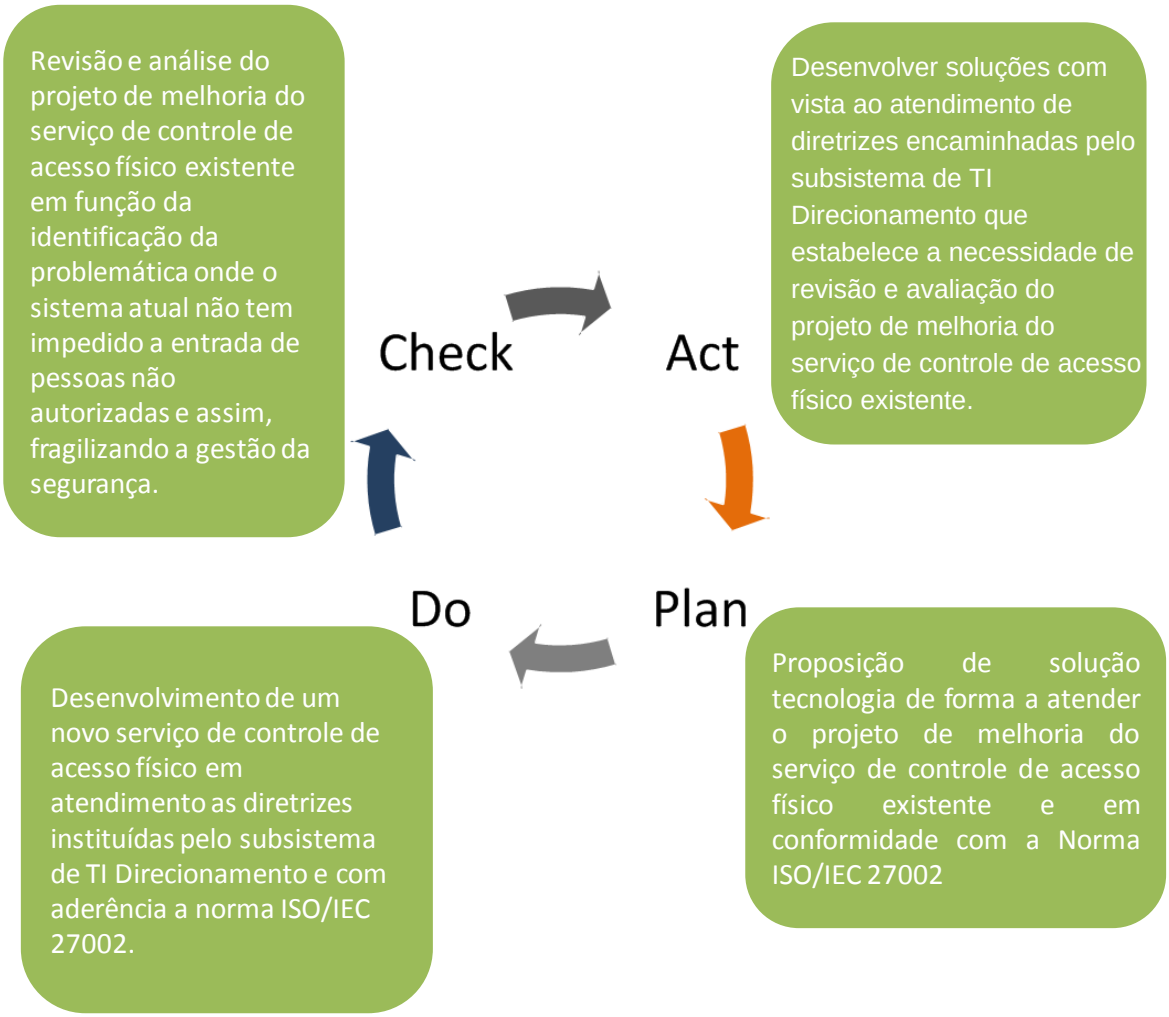


Figura 4.3 - Alinhamento com PDCA com o CGG para o subsistema de TI Desenvolvimento

4.1.4 Subsistema de TI: Entrega

O subsistema de TI, Entrega, está voltado para operação das atividades do dia a dia de acordo com as diretrizes de governança do Direcionamento e as soluções

desenvolvidas pelo Desenvolvimento. A Tabela 4.16 descreve a etapa 1 (estratégia) do CGG voltado para o subsistema de TI Entrega com foco na melhoria dos controles descritos pela Norma ISO/IEC 27002, seção 7 – Segurança física e ambiental, objetivo de controle 7.1 – áreas de segurança e controle 7.1.2 – controle para entrada física.

Sob o ponto de vista do domínio, Negócio, foram propostas estratégias para o novo serviço de controle de acesso físico que atenda as diretrizes de governança do Direcionamento e as soluções desenvolvidas pelo Desenvolvimento. Desta maneira, os conceitos sistêmicos do trio para o Negócio definem:

- Funcionalidade – executar a mesma funcionalidade referente ao controle de acesso físico descrito anteriormente;
- Processo – Estabelecer um processo de cadastramento de senha individual com a participação de cada colaborador que deve se submeter ao processo de autenticação biométrica por meio do registro da digital no novo equipamento;
- Estrutura – Operacionalizar a troca do equipamento atual pelo novo equipamento de controle de acesso físico com base na solução proporcionada pelo Desenvolvimento.

No domínio, Aplicação, é possível identificar a modificação de um dos elementos do serviço de controle de acesso por meio da solução desenvolvida pelo subsistema de TI, Desenvolvimento. Assim, os conceitos sistêmicos do trio para a Aplicação definem:

- Funcionalidade – estabelecer um novo serviço de controle de acesso físico;
- Processo – Estabelecer o processo de padronização para identificação individual;
- Estrutura – Definir a localização do novo elemento do serviço de controle de acesso (leitor biométrico).

Não se identifica a necessidade de operacionalização de projeto de alterações para o domínio, Infraestrutura, bem como para os conceitos sistêmicos Funcionalidade, Processo e Estrutura, pois não foi provisionado mudanças para esses requisitos.

Tabela 4.16 – Etapa 1 – Estratégia no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Entrega

SUBSISTEMA DE TI: ENTREGA				
ETAPA 1 - ESTRATÉGIA	NEGÓCIO	Disponibilizar o novo serviço de controle de acesso	FUNCIONALIDADE	Melhoria do serviço de controle de acesso
			PROCESSO	Estabelecer um processo de cadastramento de senha individual
			ESTRUTURA	Estabelecer um processo para troca de equipamento
	APLICAÇÃO	Modificar um dos elementos do serviço de controle de acesso (leitor biométrico)	FUNCIONALIDADE	Estabelecer um novo serviço de controle de acesso
			PROCESSO	Estabelecer o processo de padronização para identificação individual
			ESTRUTURA	Definir a localização do novo elemento do serviço de controle de acesso (leitor biométrico)
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A Tabela 4.17 apresenta no subsistema de TI Entrega a etapa 2 do CGG (Guias e coleções de melhores práticas) onde o domínio, Negócio, fundamentado pela Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o controle 7.1.2 – controle para entrada física cujo o objetivo de controle 7.1 – áreas de segurança e controle, disponibiliza seu projeto de melhoria.

Dessa maneira, os conceitos sistêmicos do trio para o Negócio definem: *i)* Funcionalidade – serviço de controle de acesso físico disponível com base na descrição do processo de melhoria contínua proposto pelo subsistema de TI, Direcionamento, e as soluções projetadas pelo subsistema de TI, Desenvolvimento; *ii)* Processo – processo de cadastramento de senha individualizada estabelecido e, por fim, *iii)* Estrutura – processo para troca de equipamento de controle de acesso físico estabelecido.

O domínio, Aplicação, estabelece a modificação de um dos elementos do serviço de controle de acesso físico (leitor biométrico) com a mesma fundamentação normativa do domínio, Negócio. Ressalta-se que os conceitos sistêmicos do trio estabelecem:

- Funcionalidade – um novo serviço de controle de acesso físico;
- Processo – um processo de padronização para identificação individual;
- Estrutura – definição da localização do novo elemento do serviço de controle de acesso (leitor biométrico).

É importante ressaltar ainda, que no domínio, Infraestrutura, não há necessidade de execução de alteração, pois a solução desenvolvida e operacionalizada não provoca mudanças nesse domínio e, respectivamente, a Funcionalidade, Processos e Estrutura não sofrem alterações.

Tabela 4.17 – Etapa 2 – Guias e coleções de melhores práticas no processo e governança e gestão da segurança nos laboratórios – Subsistema de TI Entrega

SUBSISTEMA DE TI: ENTREGA				
ETAPA 2 - GUIAS E COLEÇÕES DE MELHORES PRÁTICAS	NEGÓCIO	Disponibilizar o projeto de melhoria com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Disponibilizar a melhoria do serviço de controle de acesso com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Estabelecer um processo de cadastramento de senha individual com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Estabelecer um processo para troca de equipamento com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	Modificar um dos elementos do serviço de controle de acesso (leitor biométrico) com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Estabelecer um novo serviço de controle de acesso com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Estabelecer o processo de padronização para identificação individual com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002

			ESTRUTURA	Definir a localização do novo elemento do serviço de controle de acesso (leitor biométrico) com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

Conforme tabela 4.18, tem-se a aplicação do CGG nas etapas 3 e 4 (arquitetura atual e diagnóstico) com o foco no subsistema de TI Entrega, descreve no domínio Negócio, que em atenção as decisões determinadas pelo subsistema de TI Direcionamento e as soluções proposta pelo subsistema de TI Desenvolvimento, o projeto de melhoria do serviço de controle de acesso deve ser ponderado de forma a atender a seção 7 – segurança física e ambiental o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física descrito na Norma ISO/IEC 27002 .

Assim, é possível sugerir uma análise da melhoria do serviço de controle de acesso físico no quesito, Funcionalidade, essencialmente no acolhimento normativo. Para Processos, descreve-se a análise do processo de cadastramento de senha individual e para Estrutura decidiu-se pelo diagnóstico do processo para troca de equipamento em atendimento a norma citada.

O domínio Aplicação estabelece a reflexão sobre a modificação de um dos elementos do serviço de controle de acesso físico (leitor biométrico) com a mesma fundamentação normativa do domínio Negócio. Destaca-se que os conceitos sistêmicos do trio estabelecem:

- Funcionalidade – analisar um novo serviço de controle de acesso físico;
- Processo – analisar um processo de padronização para identificação individual;
- Estrutura – análise da definição da localização do novo elemento do serviço de controle de acesso (leitor biométrico).

No domínio Infraestrutura para os conceitos sistêmicos de Funcionalidade, Processos e Estrutura não suporta alteração, pois nesta etapa se considera a estrutura e a analise de diagnostico da situação corporativa atual.

Tabela 4.18 – Etapas 3 e 4 – Arquitetura atual (controle e monitoramento) e diagnóstico no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Entrega

SUBSISTEMA DE TI: ENTREGA				
ETAPA 3 e 4 - ARQUITETURA ATUAL (CONTROLE, MONITORAMENTO) E DIAGNÓSTICO	NEGÓCIO	Refletir sobre o projeto de melhoria com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Analisar a melhoria do serviço de controle de acesso com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Analisar o processo de cadastramento de senha individual com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Analisar o processo para troca de equipamento com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	Refletir sobre a modificação de um dos elementos do serviço de controle de acesso (leitor biométrico) com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Analisar um novo serviço de controle de acesso com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Analisar o processo de padronização para identificação individual com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Analisar a localização do novo elemento do serviço de controle de acesso (leitor biométrico) com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002

	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A tabela 4.19 apresenta a arquitetura corporativa desejada onde o domínio, Negócio, no subsistema de TI, Entrega, descreve a avaliação do projeto de melhoria no serviço de controle de acesso físico com suporte aos controles descritos pela Norma ISO/IEC 27002, seção 7 – segurança física e ambiental o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física. Os conceitos sistêmicos apontam:

- Funcionalidade – novo serviço de controle de acesso físico definido em conformidade com a norma apresentada;
- Processo – novo processo de cadastramento de senha individual definido com base na aplicação da norma de forma a estabelecer controle de acesso físico aos ambientes do laboratório;
- Estrutura – novo equipamento de controle de acesso físico definido de forma a atender aos requisitos anteriormente descritos.

O domínio, Aplicação, estabelece a avaliação sobre a modificação do serviço de controle de acesso físico (leitor biométrico) com a mesma fundamentação normativa do domínio, Negócio. Destaca-se que os conceitos sistêmicos do trio estabelecem:

- Funcionalidade – novo serviço de controle de acesso físico;
- Processo – novo processo de padronização para identificação individual;
- Estrutura – nova da localização do novo elemento do serviço de controle de acesso (leitor biométrico).

No domínio, Infraestrutura, para os conceitos sistêmicos de Funcionalidade, Processos e Estrutura não suporta alteração, pois as diretrizes estabelecidas pelo subsistema de TI Direcionamento e a solução suportada pelo subsistema de TI Desenvolvimento não contempla alteração na situação corporativa atual.

Tabela 4.19 – Etapa 5 – Arquitetura corporativa desejada no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Entrega

SUBSISTEMA DE TI: ENTREGA				
ETAPA 5 - ARQUITETURA CORPORATIVA DESEJADA	NEGÓCIO	Avaliar o projeto de melhoria com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Novo serviço de controle de acesso físico definido com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Novo processo de cadastramento de senha individual definido com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Novo equipamento de controle de acesso físico definido com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	Avaliar a modificação do serviço de controle de acesso (leitor biométrico) com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Novo serviço de controle de acesso definido com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Novo o processo de padronização para identificação individual definido com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Nova localização do novo elemento do serviço de controle de acesso (leitor biométrico) definido com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A Tabela 4.20 refere-se a etapa 6 (projeto de migração) do CGG para o subsistema de TI Entrega. No domínio do Negócio são propostos os testes de produção do

projeto de melhoria necessários para o novo serviço de controle de acesso físico com base na Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física.

Os referidos testes devem considerar nos conceitos sistêmicos: *i)* Funcionalidade – o novo serviço de controle de acesso físico; *ii)* Processo – novo processo de cadastramento de senha individual em conformidade normativa, e por fim, *iii)* Estrutura – novo equipamento de controle de acesso físico em concordância com as normas existentes.

O domínio, Aplicação, refere-se ao teste de produção necessário para a modificação do serviço de controle de acesso físico por meio da utilização de um leitor biométrico. O conceito sistêmico do trio trata:

- Funcionalidade – novo serviço de controle de acesso físico testado e verificado a aderência normativa;
- Processo – novo processo de padronização para identificação individual testado em observância as normas estabelecidas;
- Estrutura – nova da localização do novo elemento do serviço de controle de acesso (leitor biométrico) testado e aprovado.

No domínio, Infraestrutura, não foram identificadas necessidade de realização de testes de para verificação do projeto de alterações. O mesmo vale para os conceitos sistêmicos, Funcionalidade, Processo e Estrutura, pois não foi provisionado mudanças para estes componentes.

Tabela 4.20 – Etapa 6 – Projeto de migração no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Entrega

SUBSISTEMA DE TI: ENTREGA				
ETAPA 6 - PROJETO DE MIGRAÇÃO	NEGÓCIO	Teste de produção do projeto de melhoria com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Novo serviço de controle de acesso físico testado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Novo processo de cadastramento de senha individual testado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002

			ESTRUTURA	Novo equipamento de controle de acesso físico testado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	Teste de produção da modificação do serviço de controle de acesso (leitor biométrico) com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Novo serviço de controle de acesso testado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Novo o processo de padronização para identificação individual testado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Nova localização do novo elemento do serviço de controle de acesso (leitor biométrico) testado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A etapa 7 do CGG é descrita pela Tabela 4.21, no ponto de vista do subsistema de TI, Entrega, delineia no domínio, Negócio, sobre o processo de melhoria que deve ser implantado com novo serviço de controle de acesso físico com apoio na Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física. Desta maneira, os conceitos sistêmicos do trio definem:

- Funcionalidade – novo serviço de controle de acesso físico implantado e com aderência as normas relacionadas;
- Processo – novo processo de cadastramento de senha individual implantado com base normativa atendida;
- Estrutura – novo equipamento de controle de acesso físico implantado com base no projeto descrito para a modificação do equipamento de controle de acesso físico.

O domínio, Aplicação, trata da modificação do serviço de controle de acesso (leitor biométrico) deve ser implantado com aderência normativa e os conceitos sistêmico do trio considera: *i)* Funcionalidade – trata do novo serviço de controle de acesso implantado em conformidade normativa; *ii)* Processo – considera o novo processo de padronização para identificação individual implantado, e por fim, *iii)* Estrutura – nova localização do novo elemento do serviço de controle de acesso físico (leitor biométrico) implantado com referencia a norma.

Não foram identificadas necessidades de implantação de projeto de alterações para o domínio, Infraestrutura. O mesmo vale para os conceitos sistêmicos, Funcionalidade, Processo e Estrutura, pois não foi provisionado mudanças para estes elementos.

Tabela 4.21 – Etapa 7 – Implantação do projeto no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Entrega

SUBSISTEMA DE TI: ENTREGA				
ETAPA 7 - IMPLANTAÇÃO DO PROJETO	NEGÓCIO	O projeto de melhoria deve ser implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Novo serviço de controle de acesso físico implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Novo processo de cadastramento de senha individual implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Novo equipamento de controle de acesso físico implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	A modificação do serviço de controle de acesso (leitor biométrico) deve ser implantada com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Novo serviço de controle de acesso implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Novo o processo de padronização para identificação individual implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002

			ESTRUTURA	Nova localização do novo elemento do serviço de controle de acesso (leitor biométrico) implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

A etapa 8 descreve a atividade da nova arquitetura corporativa sob o ponto de vista do subsistema de TI Entrega, conforme Tabela 4.22. Para o domínio Negócio descreve-se o projeto de melhoria em produção, conforme orientado pelo subsistema de TI Direcionamento e com a solução proposta pelo subsistema de TI Desenvolvimento em observância a Norma ISO/IEC 27002, seção 7 – segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física.

A Funcionalidade neste domínio descreve o novo serviço de controle de acesso físico em atividade e em conformidade com a norma. O conceito sistêmico Processo refere-se à atividade resultante do novo processo de cadastramento de senha individual respeitando as normas destacadas. A Estrutura descreve a atividade resultante da implantação do novo equipamento de controle de acesso físico.

O domínio, Aplicação, descreve a modificação do serviço de controle de acesso físico (leitor biométrico) em atividade preservando as normas descritas anteriormente. Os conceitos sistêmicos do trio descrevem:

- Funcionalidade – novo serviço de controle de acesso físico implantado e em produção;
- Processo – novo processo de padronização para identificação individual implantada e em execução;
- Estrutura – nova da localização do novo elemento do serviço de controle de acesso (leitor biométrico) implantado e em produção observando as normas descritas.

O domínio, Infraestrutura, não se altera, pois este componente não sofreu mudanças que refletissem em seus processos, assim como para os conceitos sistêmicos, Funcionalidade, Processo e Estrutura, pois não foi provisionado execuções para estes elementos.

Tabela 4.22 – Etapa 8 – Arquitetura corporativa atual do projeto no processo de governança e gestão da segurança nos laboratórios – Subsistema de TI Entrega

SUBSISTEMA DE TI: ENTREGA				
ETAPA 8 - ARQUITETURA CORPORATIVA ATUAL (EXECUÇÃO)	NEGÓCIO	O projeto de melhoria em produção com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Novo serviço de controle de acesso físico em produção com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Novo processo de cadastramento de senha individual em produção com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Novo equipamento de controle de acesso físico em produção com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	APLICAÇÃO	A modificação do serviço de controle de acesso (leitor biométrico) em produção com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002	FUNCIONALIDADE	Novo serviço de controle de acesso implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			PROCESSO	Novo o processo de padronização para identificação individual implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
			ESTRUTURA	Nova localização do novo elemento do serviço de controle de acesso (leitor biométrico) implantado com base na seção 7, objetivo de controle 7.1 e controle 7.1.2 - ISO/IEC 27002
	INFRAESTRUTURA	Não se altera	FUNCIONALIDADE	Não se altera
			PROCESSO	Não se altera
			ESTRUTURA	Não se altera

Alinhamento com PDCA com o CGG para o subsistema de TI Entrega

O subciclo de governança envolve o processo de tomada de decisão e no CGG engloba as fases de *Check* e *Act* do PDCA.

As atividades referentes ao alinhamento podem ser descritas:

- Governança – *Check*: Para a Norma ISO/IEC 27001 o *Check* corresponde à atividade de avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do sistema de gestão da segurança da informação (SGSI) e apresentar os resultados para a análise crítica pela direção.

Resultado principal da fase *Check* na Entrega – Análise sobre a modificação de um dos elementos do serviço de controle de acesso biométrico e o processo de padronização de identificação individual dos colaboradores do laboratório.

- Governança – *Act*: Para a Norma ISO/IEC 27001 o *Act* corresponde a executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Resultado principal da fase *Act* na Entrega – Proposição da análise da troca de equipamento de controle de acesso físico com modificação de um dos elementos do serviço (leitor biométrico) com base nas diretrizes descritas pelo subsistema de TI, Direcionamento e a solução desenvolvida pelo subsistema de TI, Desenvolvimento.

O subciclo de gestão envolve o acompanhamento das atividades de execução do processo de tomada de decisão anterior e no CGG engloba as fases de *Plan* e *Do* do PDCA.

As atividades referentes ao alinhamento podem ser descritas:

- Gestão – *Plan*: Para a Norma ISO/IEC 27001 o *plan* estabelece a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

Resultado principal da fase *Plan* na Entrega – Planejar a implantação dos processos e procedimentos estabelecidos para o projeto de melhoria do serviço de controle de acesso físico de forma a atender integralmente a Norma ISO/IEC 27002, seção 7 –

segurança física e ambiental, o objetivo de controle 7.1 – áreas de segurança e controle e o controle 7.1.2 – controle para entrada física e mitigar a entrada de pessoas não autorizadas no âmbito do laboratório.

- Gestão – Do: Para a Norma ISO/IEC 27001 o *do* implementa e opera a política, controles, processos e procedimentos do SGSI.

Resultado principal da fase *Do* na Entrega – Implantação (novo serviço em produção) do projeto de melhoria do serviço de controle de acesso físico diante das diretrizes estabelecidas pelo subsistema de TI Direcionamento e a solução desenvolvida pelo subsistema de TI Desenvolvimento.

O alinhamento entre o subciclo governança, que abrange o processo de tomada de decisão descrito pelas fases *Check* e *Act* do PDCA; com o subciclo gestão, que envolve o acompanhamento das atividades de execução do processo de tomada de decisão anterior e no CGG engloba as fases de *Plan* e *Do* do PDCA, inseridos no subsistema de TI Entrega onde sua principal funcionalidade é a operação e a manutenção de serviços está representado pela Figura 4.4.

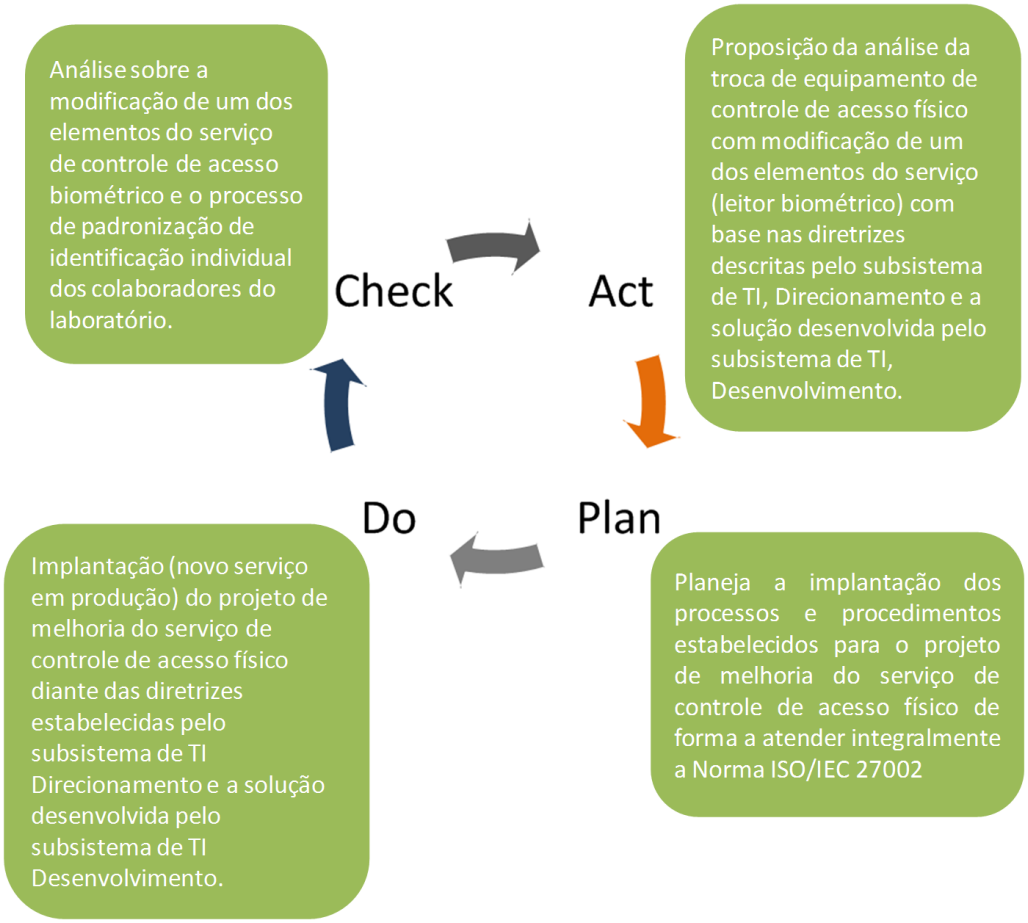


Figura 4.4 - Alinhamento com PDCA com o CGG para o subsistema de TI Entrega

Conceituação do alinhamento do CGG com o PDCA para o subsistemas de TI

A aplicação conjunta dos conceitos relativos ao ciclo de governança e gestão alinhado ao PDCA, acerca dos domínios de TI: Negócio, Aplicação e Infraestrutura para cada subsistema de TI; empreendida da análise sistêmica dos conceitos: *i)* Funcionalidade; *ii)* Processo e, *iii)* Estrutura, como fatores a serem considerados à efetivação da segurança da informação no ambiente do estudo de caso, bem como o estabelecimento de um processo de gestão da Segurança da Informação. A figura 4.5 concatena o alinhamento do CGG com o PDCA para os subsistemas de TI (Direcionamento, Direcionamento e Entrega) e apresenta os resultados encontrados na aplicação nos laboratórios.

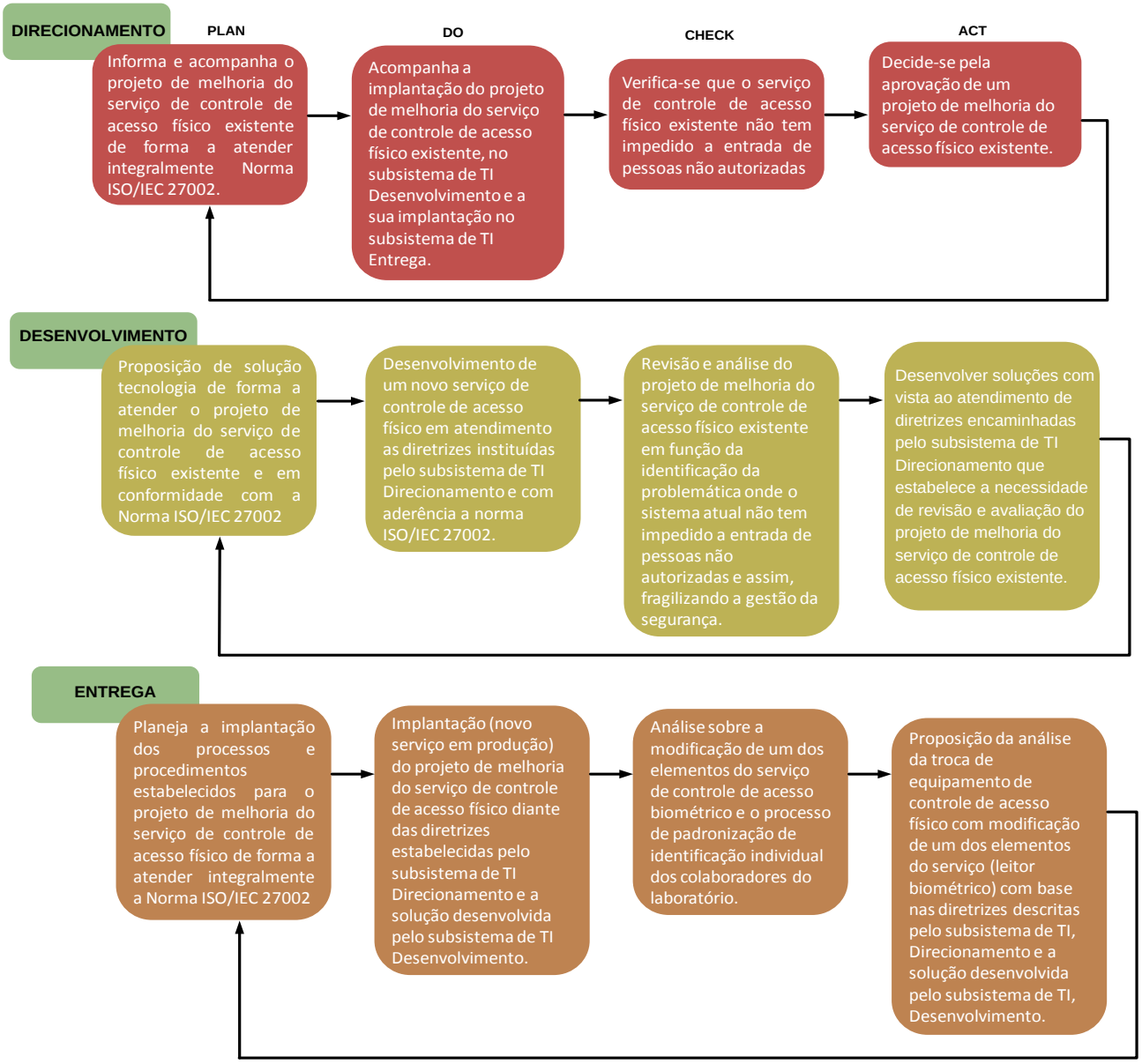


Figura 4.5 - Alinhamento do PDCA com CCG para os subsistemas de TI (Direcionamento, Desenvolvimento e Entrega)

5 CONCLUSÃO

A governança e a gestão assumem a função estratégica nas organizações de forma a prover qualidade aos negócios. Isso ocorre não apenas com foco na geração de valor, mas também em todo o processo de organização e desenvolvimento das ações de alinhamento relacionadas ao negócio almejado. Dessa forma, o processo de tomada de decisão é articulado de maneira a assumir um papel imprescindível às organizações, independente de sua estrutura ou de seu porte.

Para tanto, aprender e aperfeiçoar os conceitos de melhoria significa construir um sistema de gestão voltado ao constante aprendizado e à importância dos ativos nas organizações. O interesse das organizações pelo conhecimento relaciona-se diretamente à necessidade de superar desafios, diferenciando-se pela sabedoria e pela forma como conseguem empregar esse conhecimento [**33**].

Portanto, governar e gerenciar são ações que dependem diretamente da capacidade de compreender a organização e de a modelar de acordo com o nível de compreensão dos processos e do desenho de sua arquitetura. Quanto maior esse nível, maiores serão as possibilidades de desenho da arquitetura corporativa desejada. Isso tem como propósito a promoção e o alinhamento da organização, de acordo com as necessidades.

A organização pesquisada deve ser observada tanto globalmente como de forma particionada. A forma de visualização do todo compreende a organização como um sistema, cuja função de transferência, ou mecânica interna, só pode ser compreendida pela observação do sistema, em um caminho de fora para dentro. O entendimento sobre como usar ou controlar o sistema se dá por meio do mapeamento de funcionalidades da organização e pela descrição de seus processos, levando-se em consideração a coerência das saídas produzidas com as respectivas entradas.

A forma de visualização baseada nas partes da organização remete a uma engenharia através da qual a orientação organizacional parte de dentro para fora. O traço evidente dessa forma de visualização é o registro da perspectiva interna da organização, com foco no funcionamento dos processos existentes.

O estudo de caso em questão foi empreendido em um laboratório da Universidade

de Brasília, com a observação de suas características gerais, a coleta de dados necessária e a definição de pontos estratégicos que necessitavam passar por mudanças. Desse modo, a busca por respostas às questões propostas com relação ao modelo de arquitetura, à gestão interna da organização analisada e aos processos existentes permitiu um mais amplo entendimento da empresa analisada e consequentemente da modelagem e estruturação dos processos que a envolvem. Para tanto, foram realizadas três aplicações de conceitos sistêmicos aplicados ao ciclo de governança e gestão alinhado ao modelo PDCA.

A primeira aplicação teve como objetivo descrever a definição dos papéis organizacionais. Foi realizada em laboratório e baseou-se no entendimento de que as organizações são sistemas constituídos por outros subsistemas e nos subsistemas de TI que sofrem interação entre si de forma a permitir o alinhamento entre a TI e o negócio, descritos por: a) Direcionamento: planejamento e acompanhamento de alto nível; b) Desenvolvimento: construção de soluções e, c) Entrega: operação e manutenção de serviços. Esses subsistemas de TI descreveram o escopo de atuação na organização, assim como a identificação dos envolvidos e dos afetados, além da definição de funções e responsabilidades envolvidas.

A segunda aplicação retratou a realização de uma leitura da organização por meio dos domínios (Negócio, Aplicação e Infraestrutura) realizados para cada subsistema de TI, tratados de forma individualizada, a fim de permitir um entendimento detalhado da funcionalidade de cada subsistema. Foram incluídas as definições recorrentes para cada domínio e os principais componentes e tipos de serviços internos envolvidos, além do suporte de componentes.

Nessa etapa, foi descrito como a camada de negócios oferece produtos e serviços para clientes externos, desenvolvidos na organização por processos de negócio. A camada de aplicação apoiou a camada de negócios com serviços de aplicativos que são suportados por componentes (*software*) aplicativos. Finalmente, a camada de infraestrutura detalhou os serviços de infraestrutura disponíveis e necessários ao atendimento das camadas superiores.

Por último, foi realizada uma aplicação do conceito sistêmico do trio (Funcionalidade, Processo e Estrutura) para cada domínio (Negócio, Aplicação e Infraestrutura) inseridos em cada subsistema de TI (Direcionamento, Desenvolvimento e

Entrega). A partir da Estrutura foi possível definir os componentes e as relações necessárias para o desenvolvimento das atividades. Os Processos foram descritos com base na sequência que deveriam ser empreendidos. A Funcionalidade permitiu a definição das interações dinâmicas das atividades necessárias para produção do resultado proposto.

O processo de coleta de dados para o estudo de caso foi determinante e levou em consideração o método de leitura e a observação da rotina da organização. Tal fator permitiu a descrição do conteúdo proposto. Esta atividade pôde ser empreendida para obtenção da compreensão necessária sobre os conceitos que cercam a arquitetura corporativa atual e o desenvolvimento da arquitetura corporativa desejada. A compreensão dos processos organizacionais decorrentes da análise dos dados coletados permitiu um completo entendimento sobre o fato de que governar e gerenciar dependem, intrinsecamente, da capacidade de compreender o negócio e da modelagem proposta, a partir da utilização dos controles presentes nas normas ISO/IEC 27001 e ISO/IEC 27002. Isso por meio da concepção dos processos descritos e do desenho da nova arquitetura com base no nível de aprofundamento adotado.

A proposta do método foi realizada com base em referenciais bibliográficos e na observação da necessidade de incorporar conceitos referentes à Segurança da Informação ao escopo da Gestão de TI, de forma a permitir o entendimento organizacional e o atendimento dos requisitos de mercado. Mas, apesar de o estudo envolver conceitos referentes ao modelo PDCA, que tratam da melhoria contínua dos processos, é importante ressaltar que os resultados apresentados não contaram com um método de validação e mensuração. Esses métodos surgem como indicação para trabalhos futuros, em um entendimento completo da visão empregada. A implantação do processo de validação e de mensuração é fundamental para a verificação do comportamento da organização diante do desenho da arquitetura corporativa proposta. Acredita-se que o gerenciamento dessas condutas permitirá uma ampla contribuição ao processo de melhoria contínua dos processos inclusos no modelo PDCA.

REFERÊNCIAS BIBLIOGRAFICAS

[1] D. Moraes, *Por uma outra comunicação – Mídia, mundialização cultural e poder*. Rio de Janeiro: Record, 2004.

[2] L. P. Mello, Proposta de metodologia de gestão de riscos em ambientes corporativa na área de TI, 2008, Dissertação de Mestrado em Engenharia Elétrica - UnB.

[3] M. Gaspar, T. Gomez, and Z. Miranda, *T.I. Mudar e inovar - resolvendo conflitos com ITIL V3 - aplicado a um estudo de caso*. Brasília: Senac-DF, 2010.

[4] L. F. R Molinaro and K. H. C Ramos, *Gestão de tecnologia da informação: governança de TI: arquitetura e alinhamento entre sistemas de informação e o negócio*. Rio de Janeiro, Brasil: LTC, 2011.

[5] H. Günther, "Pesquisa qualitativa versus pesquisa quantitativa: Esta é a questão?," *Psicologia: Teoria e Pesquisa*, vol. 22, no. 2, pp. 201-210, maio-agosto 2006.

[6] R. K. Yin, *Case study research: design and methods*, 3rd ed.: Sage Publications, 2002.

[7] N. Hoppen, L. Lapointe, and E. Moreau, "Um guia para a avaliação de artigos de pesquisa em sistemas de informação," *Revista Eletrônica de Administração - REAd*, vol. 2, no. 3, novembro 1996.

[8] Leonard-Barton D., "A dual methodology for case studies: synergistic use of a longitudinal single site with replicated multiple sites," *Organization Science*, vol. 1, pp. 248-266, august 1990.

[9] A. Jensen, in Business Administration and Computer Sciense Government enterprise architecture adoption: a sistemic-discursive critique and reconceptualisation, 2010, Master's thesis for degree of Master of sciense in Business Administration and Computer Sciense - Copenhagem Business School.

[10] T. R. Gruber, "Toward principles for the design of ontologies used for knowledge

sharing," *International Journal Human-Computer Studie*, pp. 907-928, march 1993.

[11] T. Kühne, "Matters of (meta-) modelling," *In Journal on Software and Systems Modeling*, vol. 5, pp. 369-385, Apr. 2006.

[12] H. Stachowiak, *Allgemeine Modelltheorie*. Wien and New York: Springer-Verlag, 1973.

[13] W. Steinmüller, Informationstechnologie und Gesellschaft: Einführung in dieAngewandte Informatik., 1993, Wissenschaftliche Buchgesellschaft, Darmstadt.

[14] P. Weill and J. W. Ross, *Governança de TI*.: M. Books, 2006.

[15] I. Sommerville, *Engenharia de Software*, 6th ed. São Paulo: Addison Wesley, 2003.

[16] J. L. G. Dietz, *Enterprise Ontology: Theory and Methodology*. Berlin: Springer-Verlag, 2006.

[17] A. C Valença, *Aprendizagem organizacional: 123 aplicações práticas de arquétipos sistêmicos*. São Paulo: Editora Senac São Paulo, 2011.

[18] H. Kasper, O processo de pensamento sistêmico: um estudo das principais abordagens a partir de um quadro de referência proposto, 2000, Dissertação de mestrado - UFRGS.

[19] J. Gharajedaghi, *Systems thinking: managing chaos and complexity : a platform for designing business architecture*, Second Edition ed.: Elsevier, 1999.

[20] M. Lankhorst and et al., *Enterprise architecture at work: modeling, communication, and analysis*. Berlin: Springer, 2005.

[21] C. T. Betz, *Architecture and patterns for IT service management, resource planning, and governance: making shoes for the Cobbler's children*. New York: Morgan Kaufman, 2007.

[22] L. F. R. Molinaro, K. H. C. Ramos, G. Souto, and H. Abdalla Junior, "Modelo de maturidade para arquitetura corporativa de TI," *5ª conferência ibérica de sistemas y tecnologia de información*, junho 2010, Information System and Tecnologies (CISTI), 2010 5th Iberian Conference on.

[23] F. A. Garcia, Governança corporativa, 2005, Dissertação de Mestrado - UFRJ.

[24] J. Zisblat, O Impacto das Práticas ITIL na Flexibilidade Organizacional - Evidências Empíricas em uma Empresa Multinacional de TI, 2008, Dissertação de Mestrado Executivo em Gestão Empresarial - FGV.

[25] IBGC. (2011, janeiro) Instituto Brasileiro de Governança Corporativa. [Online]. http://www.ibgc.org.br

[26] C. L. Buss, Uma proposta para organização da função de TI baseada na gestão de operações, 2006, Dissertação de Mestrado - Engenharia de Produção e Sistemas - PUC/PR.

[27] N. C. Slack and R. Johnston, *Administração da produção*, 2nd ed.: Editora Altlas, 2009.

[28] J. O. A. L. Torres, Uma proposta de uma solução de BI baseado no modelo ISO/IEC 7498-4 com foco na gestão da produção de TI, 2010, Dissertação de Mestrado em Engenharia Elétrica - UnB.

[29] IT Governance Institute. (2011, março) About IT Governance. [Online]. http://www.itgi.org

[30] I. L. Magalhães, *Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL.*: Novatec, 2007.

[31] J. H. T. Júnior, J. P. Sauvé, J. A. B. Moura, and S. Q. R. Teixeira, *Redes de Computadores. Serviços, Administração e Segurança*.: Makron Books, 1999.

[32] B. Lameira, E. M. Morais, and Risoleide Freitas. (2011, janeiro) A desverticalizão

das organizações - Simpósio de Excelência em Gestão e Tecnologia - SEGeT. [Online]. http://www.aedb.br/seget/artigos06/872_A%20Desverticalizacao%20das%20Organizacoes.pdf

[33] M. Funke, "ITIL: O Lema da TI é Servir," *Informática Hoje*, no. 568, pp. 10-16, novembro 2004.

[34] L. M. A. Dória, Service profit chain, 2006, Dissertação de Mestrado - IBMEC.

[35] P. A. Mendes. (2011, fevereiro) Webinsider. Gestão de Serviços em TI e o Mundo dos Negócios, 2006. [Online]. http://webinsider.uol.com.br/2006/10/13/gestao-de-servicos-em-ti-e-o-mundo-dos-negocios/

[36] R. C. Azevedo, C. F. Bremer, D. A. N Rebelatto, and F. B. Tarallo, "Uso de ERP e CRM no suporte à gestão de demanda em ambientes de produção Make-to-Stock," *Gestão e Produção: G&P*, vol. 13, pp. 179-190, Feb. 2003.

[37] Instituto Euvaldo Lodi, Modelo de Elaboração de Plano Diretor de Tecnologia da Informação, 2008.

[38] J. S. Gubiani, M. M Braga, J. B Miranda, and J. L. Tedesco, "Inteligência de Negócios com um recurso para processo decisório," *XV SIMPEP - Simpósio de Engenharia de Produção, Bauru, Anais*, 2008.

[39] A. Calder and S. Watkins, *IT governance: a manager's guide to data security and ISO 27001 / ISO 27002*, 4th ed. London and Philadelphia: Kogan page, 2008.

[40] NBR - Associação Brasileira de Normas técnicas, ABNT NBR ISO/IEC 27001, Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos, 2007.

[41] NBR - Associação Brasileira de Normas técnicas, ABNT NBR ISO/IEC 27002 Tecnologia da informação - Código de prática para gestão da segurança de

informações, 2007.

[42] A. Calder, *Information Security based on ISO 27001/IS0 27002 - A management guide*, 2nd ed. Wilco, Amersfoort - NL: Van Haren Publishing Zaltbommel, 2009.

[43] A. Calder, *Implementing information security based on ISO 27001 / IS0 27002 - A management guide*, 1st ed. Wilco, Amersfoort - NL: Van Harem Publishing Zaltbommel, 2009.

[44] F. L. Campos, Qualidade percebida da Internet: um estudo de caso numa empresa de telecomunicações, 2005, Dissertação de Mestrado - UFF.

[45] V. F Campos, *TQC - Controle na qualidade total no estilo japonês*, 8th ed. Belo Horizonte: Bloch, 1992.

[46] A. L. Godoy. (2010, março) Centro de Desenvolvimento Profissional e Tecnológico - CEDET. [Online]. www.cedet.com.br

[47] J Boardman and B. Sauser, *Systems thinking: coping with 21st century problems*.: CRC Press, 2008.

[48] A. A. Fernandes and V. F. Abreu, *Implantando a governança de TI: da estratégia à gestão de processos de serviços*, 2nd ed. Rio de Janeiro: Brasport, 2008.

[49] A. P. Simões, Construção de uma arquitetura Técnica para melhoria da gestão de hospitais universitários federais, 2011, Dissertação de mestrado - Engenharia Elétrica - UnB.

[50] IT Governance Institute - ITGI, *Cobit 4.0: control objectives, management guidelines, maturity models*.: ITGI, 2005.

[51] W. V. Grembergen, *Strategies for information technology governance*. Hershey: Idea Group Publishing, 2004.

[52] Universidade de Brasília - UnB. (2011, junho) UnB - Universidade de Brasília.

[Online]. http://www.unb.br/sobre

[53] J. F. Lima, C. M. G. Amaral, and L. F. R. Molinaro, "Ontology: An analysis of Literature.," *Enterprise Information Systems*, pp. 426-435, 2010.

[54] L. Z. H Damázio, Avaliação dos controles Saxbox da gerência de operações de TI de uma empresa provedora de serviços de telecomunicações , 2007, Dissertação de mestrado - UnB.

[55] L. Piemonte. (2011, março) Fórum Brasileiro de Processos - ESTRATÉGIA X OPERAÇÃO: Conceitos Diferentes, Complementares e Integráveis, 2008.. [Online]. http://www.fbp.org.br/v2/artigos/GetArtigo.asp?t=ESTRATÉGIA_X_OPERAÇÃO:_CONCEITOS_DIFERENTES,_COMPLEMENTARES_E_INTEGRÁVEIS.&ID=100

[56] F. J. B. Laurindo, T Shimizu, M. M. Carvalho, and Rabechini Jr. R., "O papel da tecnologia da informação (TI) na estratégia das organizações," *Revista G&P: Gestão e Produção*, vol. 8, pp. 160-179, n. 2 2001.

[57] R. F. Silva, Uma abordagem convergente para mapeamento dos processos ITIL similares ao modelo ETOM , 2007, Dissertação de mestrado, UnB.

[58] L. F. G Soares, G. Lemos, and S. Colcher, *Redes de computadores: das LANs, MANs e WANs às redes ATM*.: Campus, 1995.

[59] L. F. R Molinaro and et al, Governance and management of information technology: decomposing the enterprise in modular building blocks based on enterprise architecture and business oriented services, 2009, Conference Enterprise Information System - CENTERIS.

[60] T. R. Gruber, "A Translation Approach to Portable Ontology Specifications," *Knowledge Acquisition*, vol. 5, no. 2, pp. 199-200, April 1993.

[61] A. N. Ferreira Neto, Metamodelos ontológicos de frameworks melhores práticas de

TI, 2009, Dissertaçao de mestrado - Universidade Católica de Brasília - UCB.

[62] T. Greenhalgh and R. Taylor, *How to read a paper: papers that go beyond numbers (qualitative research)*. Londres: BMJ Publishing Group, 1997.

[63] W. C. Rodrigues. (2011, junho) Aprendendo a pesquisar. [Online]. http://www.taciobelmonte.com.br/metodologia/wp-content/uploads/2011/04/metodologia_cientifica.pdf