VERIFICAÇÃO DE CONFORMIDADE REGULATÓRIA DOS PROCESSOS DE GOVERNANÇA DE TI: um estudo de caso de uma Empresa Pública

ÂNGELA MARIA CRISTINA CLARA

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

VERIFICAÇÃO DE CONFORMIDADE REGULATÓRIA DOS PROCESSOS DE GOVERNANÇA DE TI: um estudo de caso de uma Empresa Pública

ÂNGELA MARIA CRISTINA CLARA

ORIENTADOR: DR RAFAEL TIMÓTEO DE SOUSA JR.

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGEE. DM – 685/2017
BRASÍLIA/DF: DEZEMBRO – 2017

FICHA CATALOGRÁFICA

CLARA, ÂNGELA MARIA CRISTINA.

Verificação de conformidade regulatória dos processos de governança de TI: Um Estudo de Caso de uma empresa pública / Ângela Maria Cristina Clara – 2017.

xvii, 182p., 210 x 297 mm

Dissertação (mestrado) - Universidade de Brasília,

Faculdade de Tecnologia, Departamento de Engenharia Elétrica, 2017.

1. Governança de Tecnologia da Informação 2. Verificação de Conformidade. 3. Conformidade Regulatória 4. Elementos 5. Ações de Verificação.

I. ENE/FT/UnB II. Título (série)

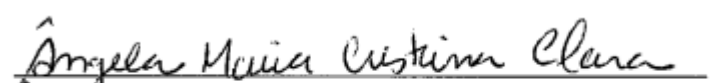
REFERÊNCIA BIBLIOGRÁFICA

CLARA, AMC (2017). Verificação de conformidade regulatória dos processos de governança de TI: Um Estudo de caso de uma empresa pública. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGEE.DM – 685/2017, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 182p.

CESSÃO DE DIREITOS

AUTOR: Ângela Maria Cristina Clara.
TÍTULO: Verificação de conformidade regulatória dos processos de governança de TI: Estudo de caso de uma empresa pública.

GRAU: Mestre ANO: 2017



ÂNGELA MARIA CRISTINA CLARA
QNM 36 CONJUNTO B CASA 34, TAGUATINGA
CEP 72.145-602 – Brasília – DF – Brasil

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

VERIFICAÇÃO DE CONFORMIDADE REGULATÓRIA DOS PROCESSOS DE GOVERNANÇA DE TI: um Estudo de Caso de uma Empresa Pública

ÂNGELA MARIA CRISTINA CLARA

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:

RAFAEL TIMÓTEO DE SOUSA JÚNIOR, Dr., ENE/UNB
(ORIENTADOR)

RICARDO STACIARINI PUTTINI, Dr., ENE/UNB
(EXAMINADOR INTERNO)

JOSÉ EDUARDO MALTA DE SÁ BRANDÃO, Dr., IPEA
(EXAMINADOR EXTERNO)

BRASÍLIA/DF, 20 DE DEZEMBRO DE 2017.

AGRADECIMENTOS

Agradeço a Deus, primeiramente, por me manter com saúde e disposição para vencer este desafio, a minha mãe pelo apoio e a minha filha Ana Clara, minha fonte de alegria e de estímulo e, também a professora e doutora Edna Canedo e ao professor e doutor Rafael Timóteo de Sousa Jr., pelo apoio na elaboração deste trabalho.

RESUMO

VERIFICAÇÃO DE CONFORMIDADE REGULATÓRIA DOS PROCESSOS DE GOVERNANÇA DE TI: Um Estudo de Caso de uma Empresa Pública.

Autora: Ângela Maria Cristina Clara

Orientador: Dr Rafael Timóteo de Sousa Jr.

Programa de Pós-graduação em Engenharia Elétrica

Brasília, 20 de dezembro de 2017

Diferentes pesquisas indicam que as empresas que possuem bons modelos de governança de TI apresentam resultados superiores em relação aos concorrentes, especialmente porque executam, de forma consistente, as melhores decisões para a TI.

Este trabalho objetiva a identificação de Elementos que Orientem as Ações de Verificação de Conformidade Regulatória – EVCR´s, visando o aprimoramento e o direcionamento da governança de TI, tendo como base as estruturas, os processos e os mecanismos que possibilitem assegurar a legalidade, a conformidade, como também apoiar nos processos de tomada de decisão da organização.

Para validar os elementos identificados como efetivamente geradores da verificação de conformidade regulatória, foi analisada a aplicação de tais elementos em uma empresa pública, prestadora de serviços de TI para todo o governo federal.

Palavras-chave: Governança de Tecnologia da Informação, Verificação de Conformidade, Conformidade Regulatória, Elementos e Ações de Verificação.

ABSTRACT

ELEMENTS CONDUCT COMPLIANCE CHECK REGULATORY ACTIONS TO IT GOVERNANCE CASE STUDY OF A PUBLIC COMPANY.

Author: Ângela Maria Cristina Clara

Advisor: Dr Rafael Timóteo de Sousa Jr.

Graduate Program in Electrical Engineering

Brasília, December 20, 2017

Different research indicates that companies that have good IT governance models feature superior results compared to competitors, especially as they perform consistently, the best decisions for IT.

This study aims to identify elements that guide regulatory compliance verification activities in order to improve and the direction of IT governance, based on the structures, processes and mechanisms that allow for ensuring the legality, compliance, as well as support the organization's decision-making processes.

To validate the elements identified as effectively generators of regulatory compliance check, the application of such elements was analyzed in a public company, a provider of IT services to the entire federal government.

Keywords: Information Technology Governance (IT), Verification of Conformity, Regulatory Compliance, Elements and Verification Actions.

SUMÁRIO

LISTA DE QUADROS

LISTA DE FIGURAS

ACRÔNIMOS E ABREVIAÇÕES

BSC – Balanced Score Card

CMDB – Configuration Manager Data Base

CMMI - Capability Maturity Management Integration

COBIT - Control Objectives for Information and Related Technology

DAC – Descrição de Atribuições e Competências

DSIC/GSI/PR – Departamento de Segurança da Informação e Comunicação – Gestão da Segurança da Informação – Presidência da República

EVCR – Elementos Orientadores da Verificação de Conformidade Regulatória na Governança de TI

IBGC – Instituto Brasileiro de Governança Corporativa

IEC - International Electrotechnical Commission

IGovTI – Índice de Governança de TI

ISACA - Information Systems Audit and Control Association

ISO - International Organization for Standardization

ITI – Instituto Nacional de Tecnologia da Informação

ITIL - Information Technology Infraestructured Library

OLA – Operational-Level Agreement

PMI - Project Management Institute

SLA – Service-Level Agreement

SLM – Service Layer Manager

SLTI/MPOG – Secretária de Logística da Tecnologia da Informação do Ministério do Planejamento e Gestão.

SMC – Serviço de Missão Crítica

TCU/SEFTI – Tribunal de Contas da União – Secretaria de Fiscalização de Tecnologia da Informação

TI – Tecnologia da Informação

1 – INTRODUÇÃO

Entende-se a Tecnologia da Informação (TI), como sendo aquela que integra estruturas e funções de acesso, transferência, armazenamento e tratamento de todas as formas da inspiração, em especial, modernamente, o texto, a voz, os dados computacionais e a imagem parada ou em movimento (WEILL E ROSS, 2005). Além dos elementos tecnológicos propriamente ditos (maquinário, algoritmos, estruturas de dados, protocolos), o termo TI abrange os processos de trabalho e a organização necessários ao usufruto dessas tecnologias pela sociedade (DE HAES E GREMBERGEN, 2006).

A tecnologia da informação (TI) tornou-se um importante fator da gestão organizacional e da obtenção de vantagem competitiva, pois tem a capacidade de agregar valor, de forma contínua, ao negócio da organização (VERHOEF, 2007).

As organizações vêm percebendo que a Tecnologia da Informação está se tornando não apenas um item de despesa significativo, mas também um dos principais ativos (VERHOEF, 2007).

Apesar de ser percebida como um dos principais ativos das organizações modernas, as decisões sobre adoção, implantação e gerenciamento de TI continuam sendo bastante complexas. Há inúmeros exemplos de empresas que fizeram elevados investimentos em projetos tecnológicos mal sucedidos, resultando em sistemas jamais concluídos ou descontinuados, e ainda, projetos nos quais as verbas e o tempo gastos em desenvolvimento excederam o planejado (PETERSON E GREMBERGEN, 2004).

Sendo um dos principais ativos, a TI pode ocasionar o comprometimento da estrutura e do funcionamento da empresa por causa de um super ou subinvestimento realizado em TI, que assim aparece como um dos principais agentes de risco nas organizações (GREMBERGEN, DE HAES E GULDENTOPS, 2004).

A monitoração dos investimentos e do gerenciamento de TI tem feito com que os executivos da área de TI e de negócio, reconheçam que o sucesso da TI, atualmente, não está na tecnologia em si, mas na forma como é governada e alinhada ao negócio (PETERSON E GREMBERGEN, 2004).

Diante dessa situação, a governança de TI aparece como uma tentativa de garantir que os investimentos em TI agreguem valor à organização ou ao negócio (DE HAES E GREMBERGEN, 2004).

De acordo com Weill e Ross (2004), as empresas que possuem bons modelos de governança de TI apresentam resultados superiores aos de seus concorrentes, especialmente porque tomam as melhores decisões sobre a TI de forma consistente.

Usufruir de recursos tecnológicos e explorá-los não é simples, mas considera-se que o mais complexo no mundo tecnológico é gerir, controlar e harmonizar a tecnologia com todos os componentes organizacionais que estão efetivamente atrelados e dependentes da Tecnologia da Informação, portanto um dos principais desafios da organização moderna é governar essa tecnologia e, por meio dela, extrair e agregar valores reais ao negócio.

Diante dessas questões, é importante questionar o que falta às organizações para estabelecerem o tão almejado controle da TI e quais os meios para implementá-lo. De acordo com Simonsson (2006a), a governança de TI pode ter três fases: compreensão, decisão e monitoração. Nas fases de compreensão e de decisão se identificam os controles que serão operacionalizados e acompanhados na fase de monitoração, permitindo verificar o quanto a TI está contribuindo para a organização e o negócio. No setor público, essa contribuição tem na conformidade regulatória um importante fator de sucesso.

Nesta dissertação é realizado um trabalho de pesquisa exploratória sobre a conformidade regulatória na governança de TI, abrangendo:

a) Artigos publicados por Henderson (1990), Venkatraman (1999), De Haes e Grembergen (2004), Simonsson (2008) e Norfolk (2011);
b) Os marcos regulatórios, como: leis, decreto, portaria, normas complementares;

c) Informações produzidas por órgãos reguladores, como os acórdãos do Tribunal de Contas da União (TCU), 1603/2008, 2308/2010 e 2585/2012;

d) E a padronização internacional, especialmente a Norma ISO/IEC 27002:2013 e os guias de melhores práticas de governança de Tecnologia da Informação como o COBIT e a ITIL.

É importante considerar, como a organização pode ter a certeza que seus processos de governança de TI estão, efetivamente, em conformidade com a legislação, com as determinações de órgãos de controle, com os padrões e melhores práticas internacionais de gestão e de governança.

As situações apresentadas relativas à governança de TI motivaram a questão de pesquisa especificamente sobre que orientações de conformidade regulatória são necessárias para assegurar a conformidade geral da governança de TI.

Com foco nessa questão de pesquisa, buscou-se identificar estruturas, processos e mecanismos de TI (Peterson, 2004), que após analisados e consolidados resultaram em elementos que orientem ações de verificação de conformidade regulatória (EVCR) em governança de TI, aplicáveis às organizações da Administração Pública Federal. As pesquisas contemplaram o levantamento de orientações de conformidade regulatória a governança de TI constantes da pesquisa bibliográfica, de leis e de determinações em acórdãos do TCU. Foi realizada, ainda, a verificação da relação destes elementos com a norma ISO/IEC 27002:2013 e os guias de melhores práticas de governança e de gestão de TI.

Sendo assim, o presente trabalho desenvolve um estudo, com base em análise documental, entrevista e verificação direta, que busca o tratamento da questão de pesquisa, objetivando contribuir para o fortalecimento das práticas de conformidade regulatória da governança de TI, de forma a melhorar os processos de tomada de decisão nas organizações.

Com intuito de demonstrar as etapas principais deste trabalho de pesquisa, as atividades foram organizadas em fases, conforme Figura 1.1.

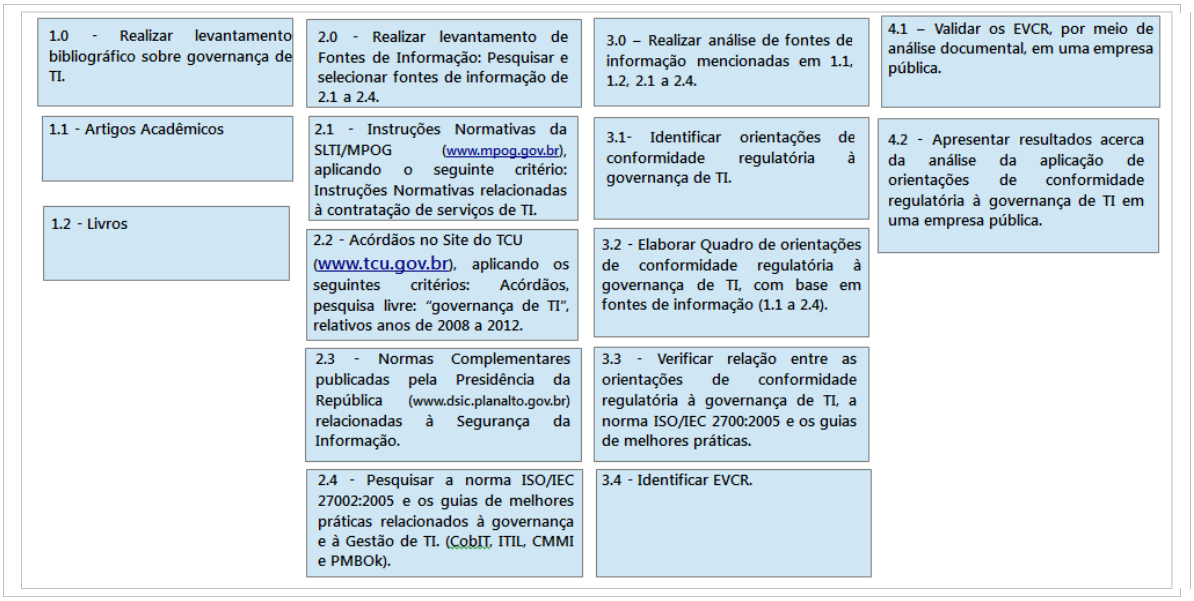


Figura 1.1 - Etapas do trabalho de pesquisa
Fonte: autoria própria

1.1 – OBJETIVOS DA PESQUISA

1.1.1 – Objetivo geral

Este trabalho propõe identificar elementos que orientem as ações de verificação de conformidade regulatória (EVCR´s) aplicáveis à governança de TI, tendo como foco os órgãos da Administração Pública Federal.

1.1.2 – Objetivos específicos

- Identificar EVCR´s com base na pesquisa bibliográfica.

- Identificar EVCR´s, considerados mandatórios, na legislação brasileira e em acórdãos do TCU.

- Verificar a relação entre os EVCR identificados na bibliografia acadêmica, na legislação brasileira com norma da Associação Brasileira de Normas Técnicas – ABNT e, também com guias de melhores práticas de gestão da TI.

- Verificar a aplicação de EVCR's associados à governança de TI em uma empresa pública.

1.2 – METODOLOGIA

Para Gil (2002), a pesquisa é um procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas propostos, sendo necessária a sua aplicação quando não se dispõe de informação suficiente para o tratamento do problema. A pesquisa pode ser desenvolvida com base em um processo que assegure a formulação adequada do problema de desenvolvimento de soluções de pesquisa e a apresentação de resultados, por meio da aplicação de métodos, de técnicas e de outros procedimentos científicos.

1.2.1 – Tipo de Pesquisa

Gil (2010) apresenta os vários aspectos metodológicos relacionados a presente pesquisa, em particular:

Após a escolha do tema deve-se realizar um levantamento bibliográfico preliminar que facilite a formulação do problema. Este levantamento bibliográfico pode ser

compreendido como um estudo exploratório, objetivando proporcionar familiaridade com a área de estudo e, assegurar que o problema seja formulado de maneira clara e precisa.

Quanto aos objetivos, esta pesquisa se classifica como exploratória. Parte significativa dos estudos exploratórios pode ser definida como pesquisas bibliográficas (Gil, 2010).

A opção pelo nível de pesquisa, como pesquisa exploratória, deu-se por meio da necessidade de buscar, de conhecer e de compreender os EVCR´s associados à governança de TI e, desta forma, contribuir para as práticas de conformidade regulatória da governança de TI, aplicadas em uma organização.

Gil (2001, p. 131) afirma que as pesquisas exploratórias têm o objetivo principal de desenvolver ideias com vista a fornecer hipóteses em condições de serem testadas em estudos posteriores. Seu planejamento reveste-se de maior flexibilidade, sendo necessária a condução de procedimentos relativamente sistemáticos para a obtenção de observações empíricas e também para a identificação das relações entre os fenômenos estudados.

As pesquisas aplicadas decorrem do desejo de conhecer com vistas a fazer algo de maneira mais eficiente ou eficaz, tendo como premissa razões de ordem prática, já a pesquisa básica tem como premissa razões de ordem intelectual.

A pesquisa objeto da presente dissertação classifica-se como aplicada, tendo como cerne a identificação de EVCR´s associados à governança de TI, constantes na pesquisa bibliográfica, na legislação, nos acórdãos do TCU e nas melhores práticas que abordam o tema governança de TI.

Os estudos realizados possibilitaram a identificação de EVCR´s na governança de TI, para que sejam observados e analisados em um contexto real e, desta forma, possam ratificar as teorias observadas da pesquisa bibliográfica ou trazer novas proposições a tais teorias.

Para a realização dos objetivos de pesquisa, foram aplicadas as seguintes abordagens: pesquisa bibliográfica, fundamentada na literatura acadêmica; análise documental; aplicação de entrevistas e de verificação direta, com base no Manual de Auditoria Operacional do Tribunal de Contas da União (TCU,2010).

A pesquisa bibliográfica foi realizada, objetivando identificar na literatura acadêmica os EVCR´s relacionados à Governança de TI.

Como parte do processo de investigação, a pesquisa documental incluiu a análise de documentos internos da organização, objeto do estudo de caso, compreendendo:

- Os normativos internos da organização relacionados aos temas: governança de TI, tecnologia da informação e segurança da informação;

- Os relatórios de verificação de conformidade da organização;

- Os documentos de atribuições e de competências das áreas de Governança de Tecnologia da Informação, de Conformidade e de Segurança da Informação;

- O mapeamento dos processos de tecnologia da informação;

- O levantamento de recomendações de órgãos de controle, direcionadas ao referido órgão, no que tange os processos de tecnologia da informação;

- As recomendações constantes de acórdãos do Tribunal de Contas da União direcionadas à organização;

A aplicação de técnica de análise documental das evidências apresentadas pela organização, com base nas legislações aplicáveis às empresas públicas, abrangendo:

– Os Marcos Regulatórios citados no subitem 3.2 desta dissertação.

– A norma ISO IEC 27002:2013 e os guias de melhores práticas relacionados à governança de TI, à tecnologia da informação e à segurança da informação.

– Base documental pública, em especial concernente à regulação de interesse para governança de TI.

– Relatórios de Auditoria do TCU, a respeito da situação da governança de TI no âmbito da Administração Pública Federal brasileira, sendo realizado o levantamento de não conformidades apontadas em relatórios de auditorias em tecnologia da informação da Secretaria de Fiscalização de Tecnologia da Informação – SEFTI, no período de 2008 a 2014 e publicados através dos acórdãos de nºs 1603/2008, 2308/2010, 1233/2012, 2585/2012 e 3117/2014, conforme citados no subitem 3.3.

1.3 – ESTRUTURA DO TRABALHO

Esta dissertação está dividida em duas partes, tendo a primeira o objetivo de apresentar a fundamentação teórica e a identificação de elementos que orientem as ações de verificação de conformidade regulatória associadas à governança de TI, aplicáveis em organizações da Administração Pública Federal brasileira. Na segunda parte da dissertação, verifica-se a aplicação de EVCR à governança de TI em uma empresa pública.

O segundo capítulo visa apresentar conceitos básicos de governança de TI e de elementos que possam orientar ações de conformidade regulatória associadas à governança de TI.

O terceiro capítulo aborda a análise de fontes de informações, objetivando a identificação de EVCR´s.

O quarto capítulo aborda a análise e discussão dos resultados acerca das verificações realizadas em uma empresa pública, com base em elementos orientem as ações de conformidade regulatória associadas a governança de TI. E, finalmente, no quinto capítulo são apresentadas as conclusões, as contribuições e recomendações de trabalhos futuros.

2 – REFERENCIAL TEÓRICO

As organizações atualmente dependem de recursos de TI para manter e suportar seus negócios, esta dependência que ocasiona a necessidade de gerir melhor seus recursos, por meio da implementação de controles que promovam a governança de TI.

O presente trabalho, no contexto do tema governança de TI, se interessa pela questão da conformidade regulatória, dedicando-se ao estudo de elementos que contribuam com a verificação de tal aspecto nos processos de trabalho relativos a TI.

Consequentemente, o referencial teórico deste trabalho está fundamentado na governança da tecnologia da informação, considerando a identificação de elementos que orientem ações de verificação de conformidade regulatória associados a tal tema.

O presente capítulo sintetiza o levantamento da literatura acadêmica relativa à Governança de TI, assim como a legislação pertinente, a padronização internacional e as melhores práticas correlacionadas ao assunto.

2.1 – GOVERNANÇA DE TI – CONCEITUAÇÃO

Embora a governança de TI seja um tópico de pesquisa relativamente novo, observa-se que diferentes definições de governança de TI, foram desenvolvidas e aprimoradas ao longo dos anos.

A seguir, a partir da pesquisa de citações de autores mais nomeados no domínio, apresenta-se um apanhado dos conceitos de TI encontrados em publicações realizadas por Norfolk (2011); Fernandes e Abreu (2010); Grembergen e De Haes (2008), Lunard et al (2007); Verhoef (2007); Simonsson (2006); Will e Ross (2005); De Haes e Grembergen (2004); ITGI (2003); Kakabadse e Kakabadse (2001); Herdenson e Venkatraman (1999); Luftman (1997); Sambamurthy e Zmud (1997) e Henderson (1990).

Henderson (1990) propôs um modelo de alinhamento estratégico em que a estratégia da TI abrange a aplicação de mecanismos e o desenvolvimento de competências sistêmicas de TI para alavancar, moldar e suportar as estratégias do negócio.

De acordo com o IT Governance Institute – ITGI (2000), a governança de TI é responsabilidade do conselho diretor e da gestão executiva, sendo parte integrante da governança corporativa e, abrangendo as lideranças, os processos e as estruturas organizacionais para garantir que a organização sustente e amplie suas estratégias e objetivos.

Assim, a governança de TI articula as lideranças, as estruturas organizacionais e os processos que asseguram que a TI da organização sustente e estenda as estratégias e objetivos do negócio, integrando e institucionalizando boas práticas (ITGI, 2003).

Para Grembergen (2002), a governança de TI é a capacidade organizacional exercida pelo conselho diretor, pelos gestores executivos e gestores da TI, para controlar a implementação da estratégia de TI, visando o alinhamento entre o negócio e a TI.

Para Weill e Ross, a governança de TI pode ser considerada um *framework* destinado a especificar os direitos de decisão e as responsabilidades de modo a encorajar comportamentos desejáveis no uso da TI (WEILL E ROSS, 2004).

Segundo Verhoef, a governança de TI é uma estrutura de relações e de processos para dirigir e governar a função da TI, dentro da organização, visando agregar valor ao negócio (VERHOEF, 2007).

Para De Haes, a governança de TI está relacionada à preocupação da alta administração em controlar o impacto estratégico da TI para o negócio (DE HAES E GREMBERGEN, 2004), pois a TI tem sido apontada como um componente crítico às organizações, principalmente no que se refere aos riscos tecnológicos.

Certamente, com relação ao impacto no negócio da organização, considera-se a possibilidade de ocorrência de incidentes relacionados a TI que podem causar prejuízo financeiro, de reputação e de imagem à organização. Assim, é importante observar que os possíveis impactos da TI no negócio, de certa forma, contribuem para que a governança de TI torne-se um assunto relevante para a alta administração (HARDY, 2006).

A governança de TI, geralmente, está presente nas organizações como parte da governança corporativa, podendo ser um mecanismo útil para se alcançar a transparência e a efetividade na gestão de recursos da TI.

De acordo com o Instituto Brasileiro de Governança Corporativa – IBGC, a governança corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre os proprietários, o conselho de administração, a diretoria e os órgãos de controle. As boas práticas de governança corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e de aperfeiçoar o valor da organização (IBGC, 2013).

Alguns trabalhos têm sugerido que a evolução da governança de TI – IBGC foi, fortemente, influenciada pela governança corporativa (PETERSON, 2004B; GREMBERGEN, 2004; ITGI, 2003). O próprio ITGI refere-se a governança de TI como sendo um subconjunto da governança corporativa (ITGI, 2003).

Segundo Simonsson, a governança de TI tem sido bastante discutida e, mesmo sendo parte da governança corporativa, tornou-se uma disciplina de seus próprios direitos (SIMONSSON, 2006).

Segundo Fernandes e Abreu (2012) a governança de TI é motivada por diversos fatores relacionados ao ambiente de negócio, como: documentos legais, integrações tecnológicas, segurança da informação e dependência do negócio em relação a TI. Todos estes motivadores da governança geram desafios relacionados a melhor forma de controlar e gerir os recursos da TI e, precisam ser tratados pela governança de TI.

Dentre estes desafios, destaca-se o alinhamento estratégico da TI e do negócio, considerado pelo ITGI (2007) como uma área de foco da governança de TI que tem por objetivo sustentar o relacionamento da TI e do negócio e, também, definir uma proposta de valor para o negócio.

2.2 – IMPLEMENTAÇÃO DA GOVERNANÇA DE TI

Em sua abordagem do tema da implementação da governança de TI, Lunardi et al (2007) destacam que:

– A decisão de implementar a governança de TI pode ser motivada pela existência de problemas críticos na organização, como a falta de recursos, ocasionando a necessidade de os executivos de TI analisarem e priorizarem seus projetos tecnológicos considerando os possíveis impactos à organização.

– Embora a discussão sobre o conceito de governança de TI tenha evoluído, de forma a torná-la mais compreensível em relação à sua importância e o seu papel na organização, a questão sobre como implementá-la tem preocupado muitos executivos e pesquisadores;

Coloca-se assim a questão de como as organizações podem pragmaticamente implementar a governança de TI. Muitos pesquisadores têm respondido a essa questão propondo que a governança de TI pode ser implementada por meio da combinação de estruturas organizacionais, de processos e de protocolos de interação, sendo necessário observar uma variedade de fatores internos e externos, por vezes conflitantes, pois as características específicas de cada organização podem demandar a aplicação de diferentes combinações desses três tipos de elementos (DE HAES E GREMBERGEN, 2006).

De acordo com Peterson (2004), na implementação da governança de TI é possível comportar as estruturas, os processos e os mecanismos de governança de TI, numa relação compreensível, em que:

- As estruturas organizacionais envolvem a existência de papéis e de responsabilidades, como aqueles dos executivos de TI e dos comitês de TI;

- Os processos abrangem o monitoramento e a tomada de decisões estratégicas;

- Os mecanismos, que podem ser tratados como protocolos de interações compreendem a participação da TI e do negócio, o diálogo estratégico, o conhecimento compartilhado e a comunicação adequada.

Quanto as ações que permeiam a estrutura organizacional da governança de TI, de acordo com Grembergen, De Haes e Guldentops (2004), o processo de implementação da Governança de TI, deve abranger os papéis, as responsabilidades e as competências da TI, considerando:

– As definições claras e inequívocas de papéis e de responsabilidades das partes envolvidas, pois é competência do conselho diretor e dos comitês a definição de papéis e de responsabilidades e, também assegurar que eles sejam compreendidos na organização.

– A formalização de papéis e de responsabilidades dos comitês, considerando que:
– O comitê diretor possui as seguintes responsabilidades específicas: acompanhar os projetos mais importantes; realizar a gestão de prioridades da TI e supervisionar os custos e a alocação de recursos da TI.

– O comitê estratégico da TI opera no nível de diretoria e o comitê gestor da TI no nível executivo.

– As competências necessárias para o desenvolvimento da governança de TI, considerando que os membros do conselho diretor mantenham seus conhecimentos atualizados acerca dos modelos de negócio, das técnicas de gestão, das tecnologias e dos riscos potenciais.

– As responsabilidades específicas do diretor presidente, como: elaborar políticas e planos estratégicos estabelecidos pelo conselho diretor; assegurar que o diretor de tecnologia da informação participe do processo de tomada de decisão e reportar-se, regularmente, ao conselho diretor, pois no processo de implementação da governança de TI, o conselho diretor exerce o papel independente de supervisor da conformidade e do desempenho do negócio.

– As responsabilidades do diretor da TI, buscando avaliar a relevância do papel do diretor da TI na implementação da governança de TI e, observando que o sucesso e a efetividade deste processo devem ser vistos como uma responsabilidade compartilhada, pois é compromisso de toda a organização manter e ampliar o valor do negócio e da TI.

– Na implementação da governança de TI, a principal preocupação do conselho diretor é a responsabilidade de governar a organização, portanto faz-se necessária a constituição de comitês estratégicos de TI e de comitês gestores de TI, considerando que os conselhos podem exercer suas funções de governança por meio de comitês.

Em relação à estrutura organizacional da TI, é importante destacar que a eficácia da governança de TI pode ser determinada pela forma como a função da TI está organizada e, também, pela posição onde a autoridade de tomada de decisão da TI está dentro da organização.

Quanto aos processos que permeiam as ações de governança da TI, é importante que o comitê estratégico da TI trabalhe em parceria com o conselho diretor e, também, com outros comitês de gestão para orientar, rever e alterar o alinhamento empresarial e a implementação das estratégias de TI.

Há também outros fatores que podem influenciar no processo de implementação da governança de TI, como os acordos de nível de serviço. Em um ambiente de governança de

TI desenvolvido, os acordos de nível de serviço (*Service-Level Agreement* – SLAs) e os respectivos processos de suporte ao gerenciamento de nível de serviço (*Service Level Management* – SLM) podem desempenhar funções importantes (DE HAES E GREMBERGEN, 2004).

Para De Haes e Grembergen (2004), as funções dos acordos de nível de serviço, compreendem:

- As definições de níveis de serviço aceitáveis pelos usuários e atingíveis pelo prestador de serviço;

- A definição de indicadores de qualidade de serviço, aceitáveis reciprocamente.

O processo de gerenciamento de nível de serviço – SLM inclui a definição de um *framework* de SLA, estabelecendo o nível de SLAs, incluindo: os serviços e as métricas correspondentes; os relatórios de monitoramento dos serviços; a revisão de SLAs e o estabelecimento de programas de melhorias.

É importante citar que um dos principais desafios da governança de TI é estabelecer que níveis de serviço devem ser expressos em termos de negócio e, também o lugar adequado dos processos de SLM e de SLA na organização (DE HAES E GREMBERGEN, 2004).

Quanto aos protocolos de interação associados a governança de TI, é importante mencionar a sua importância em situações que a organização possui as estruturas organizacionais e os processos de governança de TI, mas não funcionam adequadamente porque o negócio e a TI não trabalham conjuntamente, sendo assim necessária a aplicação destes protocolos para orquestrar e sincronizar as ações das estruturas organizacionais com os processos de governança da TI (DE HAES E GREMBERGEN, 2004).

Sendo assim, os protocolos de interação podem estar relacionados a criação de comitês, visando a participação da TI na formulação de estratégias corporativas e na elaboração de projetos de TI, o que representam ações que buscam motivar comportamentos consistentes da organização em relação a TI e, consequentemente, alinhá-los as estratégias, aos valores e a cultura organizacional (WEILL E ROSS, 2005).

Em síntese, para alcançar a governança de TI é necessário o desenvolvimento de estruturas organizacionais, de processos que apoiem, efetivamente, as ações de governança. É importante, também, avaliar a aplicação de protocolos de interação que promovam a comunicação bidirecional, a colaboração entre as equipes do negócio e da TI e a gestão do conhecimento, que podem ser atingidos por meio do revezamento profissional entre as equipes do negócio e da TI, da educação contínua e do treinamento diversificado (DE HAES E GREMBERGEN, 2004).

2.2.1 – Aspectos de Conformidade na governança de TI

A conformidade é um termo originário do verbo *to comply*, cujo sentido é agir de acordo com uma regra, um pedido ou um comando. O termo conformidade também está relacionado ao dever de cumprir, de estar em conformidade e de fazer cumprir regulamentos internos e externos impostos às atividades da organização (MORAIS, 2005).

Para Proctor (2011), a conformidade é o processo que assegura o cumprimento às políticas internas, aos procedimentos, às leis, aos regulamentos, às normas e aos acordos, podendo abranger três formas:

- Conformidade regulatória: visa assegurar o cumprimento às leis que a organização está subordinada;

- Conformidade comercial: objetiva tratar os requisitos de negócio, aplicados na organização, envolvendo as relações comerciais com os parceiros, os clientes e os fornecedores;

- Conformidade organizacional: compreende o tratamento de questões organizacionais, sendo impulsionada por ações diversas, por exemplo, a necessidade de preservar o patrimônio líquido da organização ou o desejo de demonstrar responsabilidade social corporativa.

Responder a tais necessidades, que podem ser impactadas por fatores tecnológicos é o que torna a conformidade uma preocupação crítica para as organizações.

Ainda de acordo com Proctor (2011) a implementação do processo de conformidade de uma organização, abrange os seguintes conceitos:

– No processo de conformidade, geralmente, são aplicadas as três formas de conformidade citadas anteriormente, de forma combinada, podendo gerar resultados reais à organização, como: a redução de custos e a melhoria do desempenho geral da organização;

– Na implementação do processo de conformidade, a organização é responsável pela concepção e pela gestão estratégica de tecnologias de conformidade, ou seja, tecnologias que possam apoiar os trabalhos de análise de conformidade, como também do programa de conformidade em TI.

– Quanto aos requisitos de conformidades regulatória, comercial e organizacional, são muitas vezes repetitivos – e às vezes contraditórios – entre as três formas de conformidade. Portanto, deve-se focar: no estado atual da organização em relação ao cumprimento dos requisitos de conformidade identificados; no potencial da organização para consolidar os controles de gestão e atender, efetivamente, os requisitos de conformidade e, nas oportunidades para realizar reduções de custos nos processos da organização, inclusive, nos processos de gerenciamento da conformidade.

– Em relação às estruturas de Governança de TI, os líderes da TI devem focar no estabelecimento de processos de conformidade e na divulgação das políticas para apoiá-los, sendo também os responsáveis pela seleção de tecnologias que assegurem que os

requisitos de conformidade sejam inseridos na tomada de decisão, ou seja, no processo decisório da organização, abrangendo os seguintes fatores:

- Adequação das capacidades tecnológicas às necessidades organizacionais: deve-se buscar o entendimento claro dos requisitos funcionais existentes na organização, visando identificar: as áreas que necessitam de melhoria funcional; os processos que envolvam benefícios tecnológicos; as ações necessárias para o tratamento de *gaps*; a existência de ações que possibilitem manter os líderes de TI informados sobre os processos prioritários e as decisões que envolvam a TI.

- Apoio aos processos de auditoria interna e externa: os líderes de TI devem estabelecer um processo de conformidade preventivo, buscando o alinhamento as ações de auditoria.

– Condução de iniciativas de conformidade direcionadas especificamente ao desenvolvimento de um processo de conformidade, recomenda-se que os diretores e os líderes da TI sigam cinco princípios básicos, que são:

(1) A elaboração de estratégias e de planos, visando o alinhamento aos objetivos do negócio;

(2) O desenvolvimento da governança, objetivando estabelecer um processo para a tomada de decisões e atribuir direitos de decisão, a fim de identificar e envolver as partes interessadas;

(3) A implementação de processo de gestão de mudanças baseado num sistema de comunicação para avaliar o progresso e o compromisso dos *stakeholders* em relação à gestão de mudanças;

(4) O alinhamento da conformidade com o negócio, a fim de conduzir as iniciativas de conformidade alinhadas aos objetivos de negócio da organização;

(5) O acompanhamento deve ser realizado com base em avaliações com o intuito de medir os impactos causados pelas ações de conformidade ao negócio da organização, através do *feedback* das partes interessadas. Dessas avaliações, devem-se incluir melhorias nos processos organizacionais.

É importante citar que as legislações orientam, fortemente, as ações de conformidade, portanto é fundamental compreender, acatar e gerir as legislações e as notas de orientação (NORFOLK, 2011).

2.2.2 – Aspectos de tomada de decisão na governança de TI

De acordo com Simonsson, a governança de TI está relacionada principalmente à tomada de decisão organizacional, considerando: os ativos de *hardware* e de *software* que compõem a infraestrutura tecnológica da organização; os processos da TI; as equipes e os objetivos estratégicos da TI e, principalmente, a forma como as decisões devem ser tomadas e realizadas (SIMONSSON, 2006).

A eficácia da governança de TI requer uma análise minuciosa sobre quem toma as decisões e sobre como as decisões são realizadas. Tal análise se dá em, pelo menos, cinco domínios críticos da TI, que são: os princípios, a infraestrutura, a arquitetura, os investimentos e a priorização. Desta forma, fica estabelecida uma relação entre a governança de TI e a tomada de decisão (SIMONSSON, 2006).

Segundo Simonsson (2006), a tomada de decisão associada à governança de TI consiste numa estrutura formada pelas dimensões: domínio, processo e escopo.

A dimensão domínio abrange o que as decisões devem considerar e compreende quatro unidades dimensionais:

- Objetivos: incluem as decisões relacionadas à estratégia, ao desenvolvimento e ao aperfeiçoamento das políticas da TI;

- Processos: abordam a implementação e a gestão de processos da TI, como a aquisição, o gerenciamento de nível de serviço, o gerenciamento de incidentes, e concentram-se numa estrutura de relações para desenvolver, dirigir e controlar os recursos da TI, visando atingir as metas empresariais (KORAC-KAKABADSE, KAKABADSE, 2001);

- Pessoas abrangem os papéis e as responsabilidades de diferentes *stakeholders;* e

- Tecnologias: representam as coisas físicas que as decisões consideram, como o hardware, os softwares e a infraestrutura tecnológica (SIMONSSON, 2006).

Segundo Simonsson (2006a), no que se refere a definição de governança de TI associada ao processo de tomada de decisão, pode ser representada, conforme apresentado na figura 2.1 (SIMONSSON, 2006a).

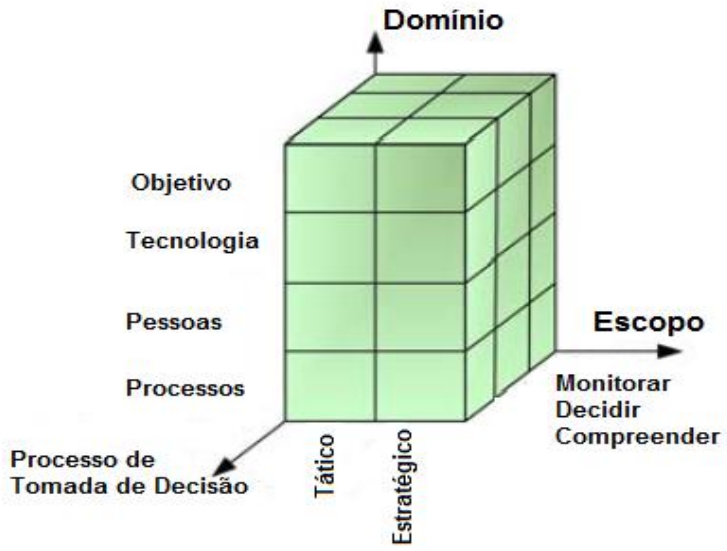


Figura 2.1- Processo de Tomada de Decisão na Governança de TI

Fonte: Simonsson (2006a, p. 9), traduzida e adaptada.

Com intuito de proporcionar melhor entendimento em relação à aplicação das dimensões e, suas respectivas unidades dimensionais sendo realizado o levantamento de palavras-chave objetivando delimitar cada dimensão conforme apresentado no Quadro 2.1.

Quadro 2.1 – Exemplos de palavras-chave relativas aos domínios de tomada de decisão na governança de TI.

Fonte: autoria própria

Dimensão	Unidade Dimensional	Palavras-chave relacionadas às unidades dimensionais
Domínio	Objetivo	Política, documento estratégico, metas, *roadmap*, princípios.
	Processo	Atividades, processos, procedimentos.
	Pessoas	Papéis, responsabilidades, grupos de *stakeholders*, estrutura corporativa.
	Tecnologia	Infraestrutura, arquitetura, servidores, aplicações.
Processo	Entender	Análise cuidadosa, entender a organização, avaliação e planejamento da tomada de decisão.
	Decidir	Dirigir, coordenar, alinhar o processo de tomada de decisão com fatores externos, autoridade de decisão.
	Monitorar	Controle, *frameworks* de controle, auditoria, responsabilidade.
Escopo	Tático	Gestão de nível inferior, linha de tempo curta, gestão da divisão de TI.
	Estratégico	Gestão de alto nível, efeitos em longo prazo, operações diárias.

Segundo Simonsson (2008), é importante assegurar que a governança de TI não seja projetada apenas para alcançar a eficiência interna da TI, mas também almejar a implantação de bons processos organizacionais apoiados pela TI, pois o objetivo de uma boa governança de TI é prover o negócio com o melhor suporte necessário. Nesse contexto, o processo de tomada de decisão abrange três fases: compreensão, decisão e monitoração. Nestas fases são tratadas as relações entre o negócio e a TI, ou seja, o mundo real e o dia a dia usados para tomada de decisão.

Na fase de compreensão do processo de tomada de decisão antes de decidir questões relacionadas à TI, a organização deve ser claramente compreendida. Os fatos têm que ser pensados, investigados e transformados em um modelo de apoio a tomada de decisão, que pode ser um mapa cognitivo (SIMONSSON, 2006a).

Na fase de decisão, uma vez que o modelo de apoio à tomada de decisão é criado, a decisão real pode ser feita de acordo com os princípios corporativos da TI, em tempo hábil e pelas pessoas certas, sendo considerado, ainda, nesta fase o planejamento de como tomar a decisão (LAGERSTRÖM, 2005).

Na fase de monitoramento do processo de tomada de decisão, a decisão deve ser acompanhada e monitorada, através da implementação de elementos de controle para cada processo, visando avaliar o desempenho com base em situações reais.

No processo de tomada de decisão, o escopo deve ser considerado, pois existem os aspectos de longo e de curto prazo para cada decisão realizada. O escopo pode ser usado para distinguir entre diferentes níveis de tomada de decisão, considerando que uma decisão estrategicamente importante pode exigir mais preparação que uma decisão tática (SOHAL, 2002).

Em síntese, a efetividade do processo de tomada de decisão depende da aplicação de mecanismos que assegurem o acompanhamento e a monitoração contínua deste processo (SIMONSSON, 2006).

Outro ponto de vista sobre o tema é apresentado por Weill e Ross (2005), com foco nas decisões chave da governança de TI abrangem cinco domínios de decisão, que são:

a) Os princípios da TI que compreendem as decisões estratégicas sobre o papel estratégico da TI no negócio;

b) A arquitetura de TI que consiste em um conjunto de opções técnicas para orientar a organização em relação às necessidades do negócio;

c) A infraestrutura da TI que abrange as capacidades funcionais da TI na organização;

d) O levantamento das necessidades do negócio, em relação aos aplicativos da TI adquiridos ou desenvolvidos internamente; e

e) Os investimentos em TI, a priorização e as decisões de investimento que determinam quanto e onde investir na TI.

Cada domínio de decisão pode ser abordar os seguintes níveis: corporativo, unidade de negócios ou funcional ou uma combinação dos três domínios, sendo que o primeiro passo é determinar os papéis e as responsabilidades para cada área de decisão (WEILL E ROSS, 2005).

Quanto as abordagens de tomada de decisões relativas a TI, tais fatores identificam arquétipos que vão desde as abordagens fortemente centralizadoras àquelas fortemente descentralizadoras:

a) Monarquia do negócio: abordagem mais centralizada, onde um executivo sênior ou um grupo de executivos seniores, eventualmente incluindo o diretor da TI, decidem as questões relacionadas a TI.

b) Monarquia da TI: as decisões são tomadas pelo executivo de TI ou por um grupo de executivos da TI.

c) Sistema federal: os executivos, os representantes das unidades organizacionais e todos os grupos operacionais colaboram com o departamento de TI.

d) Duopólio da TI: abordagem envolve executivos de TI e um grupo de líderes que representam as unidades operacionais.

e) Sistema feudal: unidade de negócio ou os líderes de processo decidem, de forma isolada, com base nas necessidades do negócio ou dos processos da organização.

f) Anarquia: representa o sistema mais descentralizado, em que cada usuário individualmente ou em pequenos grupos busca sua própria TI.

De acordo com Weill e Ross (2005), uma vez que os arquétipos para tomada de decisão são mapeados, a organização deve elaborar e implementar um conjunto coordenado de mecanismos de governança. As organizações, geralmente, projetam três tipos de mecanismos de governança:

- As estruturas de tomada de decisão – nas estruturas de tomada de decisão, os mecanismos de governança de TI mais visíveis são os comitês e os papéis organizacionais que posicionam os responsáveis pela tomada de decisão de acordo com os arquétipos pretendidos (WEILL E ROSS, 2005).

- Os processos de alinhamento: os processos de alinhamento são técnicas de gestão para garantir a participação ampla e efetiva nas decisões e nas implementações da governança de TI (WEILL E ROSS, 2005).

- As comunicações formais: as comunicações formais são necessárias ao processo de tomada de decisão, pois a ausência de comunicação pode criar barreiras para uma governança de TI eficaz, pois elas podem representar a falta de entendimento sobre como as decisões são tomadas, quais processos estão sendo implementados e quais os resultados desejados. A gestão do processo de comunicação da governança de TI pode ocorrer através das seguintes ações: publicações de anúncios gerais; instituição de comitês formais; comunicações realizadas periodicamente, pelo diretor da TI ou pela área de governança de TI (WEILL E ROSS, 2005).

2.2.3 – Guia de melhores práticas que abordam a governança de TI

Guias de melhores práticas vêm sendo desenvolvidos por entidades profissionais, visando tornar os processos de trabalho das organizações mais transparentes, inteligíveis,

controláveis e confiáveis. Dentre os guias de melhores práticas relacionados à governança e a gestão de TI, é possível mencionar: o PMBOK, o COBIT, a ITIL e o CMMI, a seguir apresentados.

2.2.3.1 – *Control Objectives for Information and related Technology - COBIT*

O COBIT é um dos *framework*s mais conhecido para avaliações de maturidade da governança de TI (ITGI, 2005; Guldentops, 2004; Grembergen, 2008). Sua primeira versão foi publicada pelo ITGI em 1998 (COBIT 5, 2012). Encontra-se, atualmente, na versão 5 publicada em abril de 2012 pela ISACA, que oferece um *framework* abrangente visando auxiliar as organizações nos processos de governança e de gestão da TI (COBIT 5, 2012).

O COBIT 5 pode ser útil para organizações pequenas ou grandes, sejam comerciais ou do setor público, a sua aplicação é realizada por meio de um *framework* integrado que pode abranger toda a organização (COBIT 5, 2012).

O framework do COBIT 5 tem base em cinco princípios-chave, voltados à governança e à gestão de TI da organização, sendo:

- Princípio 1: reunir as necessidades dos s*takeholders:* de acordo com o COBIT 5, as organizações existem para criar valor, mantendo um equilíbrio entre os benefícios e a otimização de risco em relação ao uso de recursos da TI.

- Princípio 2: cobrir a organização fim a fim: o *COBIT* 5 integra a governança corporativa da TI na organização, abrangendo todas as funções e processos internos da organização.

- Princípio 3: aplicar um framework único e integrado: existem vários padrões relacionados a TI, cada padrão fornece orientações sobre um subconjunto de atividades da TI. O *COBIT* 5 busca a aplicação de um *framework* único para a governança e a gestão corporativa da TI.

- Princípio 4: possibilitar uma abordagem holística: o COBIT 5 propõe a aplicação de uma abordagem holística com base na eficiência e na eficácia da governança e da gestão corporativa da TI, considerando os vários componentes que interagem neste contexto. O COBIT 5 define ainda um conjunto de facilitadores para apoiar a implementação de um sistema de governança e de gestão corporativa da TI, definindo sete categorias de facilitadores: os princípios, políticas e f*rameworks; o*s processos; as estruturas organizacionais; a cultura, a ética e o comportamento; as informações; os serviços, a infraestrutura e as aplicações; as pessoas; as habilidades e as competências.

- Princípio 5: separar a governança e a gestão da TI: o *framework COBIT* 5 faz uma clara distinção entre a governança e a gestão da TI, pois estas disciplinas abrangem diferentes tipos de atividades, exigem diferentes estruturas organizacionais e servem a propósitos diferentes.

É importante citar que o COBIT 5, abrange controles e objetivos de controles do COBIT 4.1, entre os quais um modelo de maturidade para governança de TI, que segue os mesmos princípios da maturidade do *software engineering institute capability model – CMMI* também fornece uma definição de governança de TI consistindo em quatro domínios:

– O domínio planejar e organizar (PO) abrange 10 processos estratégicos e táticos de TI, relativos a identificação da forma como a TI pode melhor contribuir para a consecução dos objetivos do negócio.

– O domínio adquirir e implementar (AI) abrange os sete processos que se preocupam com a aquisição e a implementação de produtos e serviços de TI.

– O domínio entrega e suporte (DS) está relacionado a entrega de serviços necessários, a gestão de segurança e continuidade, o suporte de serviços para os usuários, o gerenciamento de dados e as instalações operacionais.

– O domínio monitorar e avaliar (ME) aborda a gestão de desempenho, o monitoramento do controle interno, a conformidade regulatória e a governança, considerando que os processos da TI precisam ser periodicamente avaliados para assegurar a qualidade e a conformidade com os requisitos de controle.

Os domínios definem 34 processos e cada processo contém uma série de indicadores de maturidade de governança de TI, como: as atividades, os documentos, as métricas e o suporte para os papéis e as atribuições de responsabilidade.

Em artigo publicado em 2006, Simonsson apresentou os resultados obtidos por meio da aplicação do COBIT em testes de aplicabilidade relacionados a governança de TI em uma organização. Em 2008, na sua tese, aplicou o conceito de governança de TI como um conjunto de processos, de atividades, de papéis, de documentos e de métricas adaptados ao COBIT.

No contexto deste trabalho as práticas recomendadas no COBIT tornam-se necessárias na análise de questões relativas à Governança e à Gestão da TI apontadas nos EVCR´s identificados na Literatura Acadêmica. Vale citar que os domínios e os processos do COBIT são aplicados pelos órgãos de fiscalização e controle em trabalhos de auditoria, por meio de recomendações, especificamente, do Tribunal de Contas da União no âmbito da administração Pública Federal Brasileira, sendo que tais ações visam contribuir para o fortalecimento da aplicação de melhores práticas nas organizações Brasileiras.

2.2.3.2 – *Information Technology Infrastructure Library - ITIL*

A ITIL é uma biblioteca de infraestrutura de TI que pode auxiliar na criação de processos relacionados à entrega e ao suporte de serviços. A ITIL também detalha o

estabelecimento e a manutenção de acordos de nível de serviço (SLA) e de acordos de nível de operação (OLA). As práticas recomendadas na ITIL tornam-se necessárias na análise de questões relativas a gestão de serviços de TI, possivelmente, identificadas em EVCR´s da literatura acadêmica. Além de proporcionar o alinhamento entre os EVCR´s e esta melhor prática.

2.2.3.3 – *Project Management Body of Knowledge - PMBOK*

O PMBOK é uma metodologia de gerenciamento de projetos baseada nos princípios preconizados pelo *Project Management Institute* (PMI), de acordo com o Guia PMBOK 5ª edição. O gerenciamento de projetos, na visão do PMI, identifica e descreve as principais áreas de conhecimento, grupos de processos e boas práticas. O gerenciamento de projetos é realizado por meio da aplicação e integração de 47 processos de gerenciamento de projetos agrupados em cinco grupos de processos. Esses cinco grupos de processos são: início, planejamento, execução, monitoramento e controle e encerramento.

Um ponto importante do uso desta metodologia é que a equipe do projeto é responsável por identificar, no início do projeto, quais processos de gestão são necessários e devem ser executados tendo em vista a circunstância específica e exclusiva que caracteriza cada projeto. A não execução de processos definidos como importantes afetará negativamente o projeto, pois o projeto é um esforço integrado. Por exemplo, uma mudança de escopo quase sempre afeta o custo do projeto. Outro exemplo clássico são projetos que exigem esforço e investimento extra de comunicação com as partes envolvidas, cujos interesses seriam afetados negativamente pela execução ou pelos resultados do projeto caso não houvesse um trabalho antecipado de convencimento e negociação.

As áreas de conhecimento de gerenciamento são: Gerenciamento de Integração do Projeto, Gerenciamento do Escopo do Projeto, Gerenciamento do Tempo do Projeto, Gerenciamento dos Custos do Projeto, Gerenciamento da Qualidade do Projeto,

Gerenciamento dos Recursos Humanos do Projeto, Gerenciamento das Comunicações do Projeto, Gerenciamento dos Riscos do Projeto, Gerenciamento de Aquisições do Projeto e Gerenciamento das Partes Interessadas no Projeto.

Estes processos de comunicação precisam ser identificados como necessários e devidamente planejados de forma integrada com os demais processos de trabalho do projeto. Assim, serão realizadas atividades relativas ao:

- Gerenciamento da Integração do Projeto: abrange os processos necessários para assegurar que os diversos elementos do projeto sejam adequadamente coordenados. A integração envolve tomada de decisão e escolhas diretamente ligadas aos objetivos do projeto e aos processos das etapas de desenvolvimento e execução do plano do projeto, assim como ao processo de controle de alterações. O gerenciamento da integração é composto pelos processos: desenvolver o termo de abertura do projeto, desenvolver o plano de gerenciamento do projeto, orientar e gerenciar, monitorar e controlar, realizar o controle integrado de mudanças e encerrar o projeto ou fase.

- Gerenciamento do Escopo do Projeto: este gerenciamento descreve os processos necessários para assegurar que o projeto contemple todo o trabalho requerido, e nada mais que o trabalho requerido, para completar o projeto com sucesso. A preocupação fundamental deste gerenciamento compreende definir e controlar o que está ou não, incluído no projeto, sendo composto pelos processos: planejar o gerenciamento do escopo, coletar os requisitos, definir o escopo, criar a EAP, validar o escopo e controlar o Escopo.

- Gerenciamento do Tempo do Projeto: abrange os processos necessários para assegurar que o projeto termine dentro do prazo previsto, sendo composto pelos processos: planejar o gerenciamento do cronograma, definir as atividades, sequenciar as atividades, estimar os recursos das atividades, estimar as durações das atividades, desenvolver o

cronograma e controlar o cronograma. o correto gerenciamento do tempo do projeto é imprescindível para o sucesso do projeto.

- Gerenciamento dos Custos do Projeto: o gerenciamento dos custos do projeto inclui os processos envolvidos em planejamento, estimativas, orçamentos, financiamentos, gerenciamento e controle dos custos, de modo que o projeto possa ser terminado dentro do orçamento aprovado, sendo composto pelos processos: Planejar o Gerenciamento dos Custos, Estimar os Custos, Determinar o Orçamento e Controlar os Custos. No projeto, várias atividades afetam os custos do projeto e desta forma, o planejamento e controle dos custos são fundamentais.

- Gerenciamento da Qualidade do Projeto: o gerenciamento da qualidade do projeto inclui os processos e as atividades da organização executora que determinam as políticas de qualidade, os objetivos e as responsabilidades, de modo que o projeto satisfaça às necessidades para as quais foi empreendido. O gerenciamento da qualidade do projeto usa as políticas e procedimentos para a implementação, no contexto do projeto, do sistema de gerenciamento da qualidade da organização e, de maneira apropriada, dá suporte às atividades de melhoria contínua do processo contínuo. O gerenciamento da qualidade do projeto objetiva garantir que os requisitos do projeto, incluindo os requisitos do produto, sejam cumpridos e validados, sendo composto pelos processos: Planejar o Gerenciamento da Qualidade, Realizar a Garantia da Qualidade e Realizar o Controle da Qualidade.

- Gerenciamento dos Recursos Humanos do Projeto: o Gerenciamento dos Recursos Humanos do Projeto inclui os processos que organizam, gerenciam e guiam a equipe do projeto. A equipe do projeto consiste de pessoas com papéis e responsabilidades designadas para realizar o projeto. Os membros da equipe do projeto podem ter vários conjuntos de habilidades, atuar em regime de tempo integral ou parcial, e podem ser acrescentados ou removidos da equipe à medida que o projeto progride. Sendo composto

pelos processos: desenvolver o plano dos recursos humanos, mobilizar a equipe do projeto, desenvolver a equipe do projeto e gerenciar a equipe do projeto.

- **Gerenciamento das Comunicações do Projeto**: O gerenciamento das comunicações do projeto inclui os processos necessários para assegurar que as informações do projeto sejam planejadas, coletadas, criadas, distribuídas, armazenadas, recuperadas, gerenciadas, controladas, monitoradas e finalmente disponibilizadas de maneira oportuna e apropriada. Os gerentes de projeto passam a maior parte do tempo se comunicando com os membros da equipe e outras partes interessadas do projeto. A comunicação eficaz cria uma ponte entre as diversas partes interessadas do projeto, diferentes níveis de conhecimento, e diversas perspectivas e interesses que podem impactar ou influenciar a execução ou resultado do projeto.

É importante mencionar que a gestão da comunicação é frequentemente ignorada pelos gerentes de projeto, no entanto nos projetos concluídos com sucesso o gerente consome 90% do seu tempo envolvido com algum tipo de comunicação (formal, informal, verbal, escrita). Este gerenciamento abrange os processos: planejar o gerenciamento das comunicações, gerenciar as comunicações e controlar as comunicações.

- **Gerenciamento dos Riscos do Projeto**: o gerenciamento dos riscos do projeto inclui os processos de planejamento, identificação, análise, planejamento de respostas e controle de riscos do projeto. Os objetivos do gerenciamento dos riscos do projeto são aumentar a probabilidade de eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto. Este gerenciamento inclui os processos: planejar o gerenciamento dos riscos, identificar os riscos, realizar a análise qualitativa dos riscos, realizar a análise quantitativa dos riscos, planejar as respostas aos riscos e controlar os riscos.

– **Gerenciamento de Aquisições do Projeto**: o gerenciamento das aquisições do projeto inclui os processos necessários para comprar ou adquirir produtos ou serviços ou resultados externos à equipe do projeto e abrange os processos: gerenciamento de contratos e controle de mudanças que são necessários para desenvolver e administrar contratos ou pedidos de compra emitidos por membros autorizados da equipe do projeto, como também a administração e gestão dos contratos do projeto.

- Gerenciamento das Partes Interessadas do Projeto: o gerenciamento das partes interessadas do projeto inclui os processos exigidos para identificar todas as pessoas, grupos ou organizações que podem impactar ou serem impactados pelo projeto, analisar as expectativas das partes interessadas e seu impacto no projeto, e desenvolver estratégias de gerenciamento apropriadas para o engajamento eficaz das partes interessadas nas decisões e execução do projeto. O gerenciamento das partes interessadas também se concentra na comunicação contínua com as partes interessadas para entender suas necessidades e expectativas, abordando as questões conforme elas ocorrem, gerenciando os interesses conflitantes e incentivando o comprometimento das partes interessadas com as decisões e atividades do projeto.

No contexto deste trabalho as práticas recomendadas no PMBOK tornam-se necessárias na análise de questões relativas a gestão de projetos possivelmente identificadas por meio de EVCR´s da literatura acadêmica. Além de proporcionar o alinhamento entre os EVCR´s e esta melhor prática.

2.2.3.4 – CMMI - *Capability Maturity Model Integration*

O CMMI é um Modelo Integrado de Maturidade e de Capacidade para Melhoria de Processos, destinado ao desenvolvimento de produtos e de serviços, é composto pelas melhores práticas associadas às atividades de desenvolvimento e de manutenção que cobrem o ciclo de vida do produto desde a concepção até a sua entrega e manutenção (CMMI, 2010).

O objetivo do CMMI é auxiliar as organizações na melhoria de seus processos de desenvolvimento e de manutenção de produtos e de serviços, permitindo a geração de diversos modelos, treinamentos e métodos de avaliação para áreas de interesse específicas, sendo considerado um modelo de referência para organizações em muitos setores, como: aeroespacial, bancário, *hardware* de computador, *software*, defesa, indústria automobilística e telecomunicações (CMMI, 2010).

Os modelos que fazem parte do CMMI para o desenvolvimento de software contêm práticas que cobrem a gestão de projeto, a gestão de processos, a engenharia de sistemas, a engenharia de hardware, a engenharia de software e outros processos de suporte utilizados no desenvolvimento e na manutenção de software. O modelo CMMI abrange também a aplicação de equipes integradas para atividades de desenvolvimento e de manutenção de software (CMMI, 2010).

No contexto deste trabalho as práticas recomendadas no CMMI tornam-se necessárias na análise de questões relativas ao desenvolvimento de software, possivelmente, identificadas por meio de EVCR´s da literatura acadêmica. Além de proporcionar o alinhamento entre os EVCR´s e esta melhor prática.

2.2.3.5 – Norma ISO/IEC 27002:2013

A norma ABNT NBR ISO/IEC 27002:2013 define os requisitos para implementação de um Sistema de Gestão da Segurança da Informação (SGSI) e aborda os seguintes temas:

a) Política de Segurança da Informação
b) Orientação da direção para a segurança da informação.
c) Responsabilidades e Papéis para a Segurança da Informação.
d) Segregação de Funções.
e) Segurança da Informação no Gerenciamento de Projetos.
f) Dispositivos móveis e trabalho remoto.

g) Gestão de ativos.

h) Classificação da Informação.

i) Segurança em recursos humanos.

j) Segurança física e do ambiente.

k) Gestão das operações e comunicações.

l) Controle de acesso.

m) Aquisição, desenvolvimento e manutenção de sistemas de informação.

n) Gestão de incidentes de segurança da informação.

o) Gestão da continuidade do negócio.

p) Conformidade.

q) Controle Criptográfico.

É importante citar que, nessa norma, cada categoria principal da segurança da informação contém um objetivo de controle que define o que deve ser alcançado e os controles que podem ser aplicados para atingir esse objetivo de controle. As descrições dos controles estão estruturadas da seguinte forma:

- Controle: define qual o controle específico para atender ao objetivo de controle.

- Diretrizes para implementação: contempla informações mais detalhadas para apoiar a implementação do controle e atender ao objetivo de controle e informações adicionais. Contém informações que podem ser consideradas, como por exemplo, considerações legais e referências a outras normas.

Em síntese, a norma NBR ISO/IEC 27002:2013 pode ser considerada como um ponto de partida para o desenvolvimento de diretrizes específicas para a organização no que se refere a implementação de controles relacionados à segurança da informação.

No contexto deste trabalho a Norma ISO/IEC 27002:2013 torna-se necessária para que os controles relativos a segurança da informação que são relevantes à Governança de Tecnologia da informação, sejam considerados na análise dos EVCR´s identificados na

literatura acadêmica. Além de proporcionar o alinhamento entre os EVCR´s e esta melhor prática.

É importante citar que os controles desta norma são aplicados pelos órgãos de fiscalização e controle em trabalhos de auditoria, por meio de recomendações, especificamente, do Tribunal de Contas da União no âmbito da Administração Pública Federal Brasileira, sendo que tais ações visam contribuir para o fortalecimento da aplicação de melhores práticas nas organizações Brasileiras.

2.3 SINTESE DO CAPÍTULO

O objetivo deste capítulo foi apresentar o resultado da revisão dos principais conceitos de Governança Corporativa e de Governança de TI. Sendo abordado ainda, a aplicação do *compliance*, com base na literatura acadêmica e melhores práticas de Tecnologia da Informação e de Segurança da Informação voltada para a conformidade regulatória dos processos de governança de TI e o que esta conformidade pode agregar às Organizações, como fortalecimento da Governança e a melhoria dos processos de decisão. Por fim, os conceitos apresentados relativos à Governança de TI, na literatura acadêmica e nas melhores práticas, serão aplicados na seleção de elementos que orientem ações de verificação de conformidade regulatória – EVCR´s na literatura acadêmica, abordados no próximo capítulo.

3 – SELEÇÃO DOS EVCR´s PERTINENTES

Neste capítulo serão apresentados elementos que orientem ações de verificação de conformidade regulatória – EVCR´s. Sendo que, de acordo com a literatura acadêmica, estes elementos representam Estruturas, Processos e Mecanismos determinantes à governança de TI que podem contribuir na implementação ou no fortalecimento desta na organizações.

As fontes de informação que possibilitaram a seleção de EVCR´s na literatura acadêmica, incluíram: livros e artigos acadêmicos relativos ao tema Governança e gestão de TI.

Diante da identificação de EVCR´s foi realizada a busca de informações que estivessem alinhadas aos EVCR´s, em Marcos Regulatórios da legislaçaõ brasileira, bases de dados digitais do Tribunal de Contas da União – TCU, na Norma ISO/IEC 27002:2013 e, também nas melhores práticas de Governança e de Gestão de TI.

A coleta e a análise de informações seguiram a ordem de busca:

a) na revisão da literatura acadêmica;

b) nos Marcos Regulatórios;

c) nos acórdãos do TCU; e

d) na Norma ISO/IEC 27002:2013 e nos guias de melhores práticas, como: COBIT, ITIL, CMMI e PMBOK.

A análise possibilitou a identificação de Estruturas, Processos e Mecanismos de Govrnança que resultaram nos EVCR´s, conforme Quadro 3.7 – Síntese dos EVCR´s associados à governança de TI.

3.1 – EVCR´s IDENTIFICADOS NA PESQUISA BIBLIOGRÁFICA

As pesquisas bibliográficas realizadas em artigos e livros acadêmicos especialmente Norfolk (2011), Simonsson (2008), De Has e Grembergen (2004), Obrien (2004), Peterson (2004), Duffy (2002), ITGI (2001), Kaplan e Norton (1992), possibilitaram identificar os EVCR´s apresentados no Quadro 3.1.

A identificação de EVCR´s deu-se por meio de pesquisa em artigos e livros acadêmicos, por meio da aplicação do critério de busca de expressões sobre elementos necessários à governança de TI com os seguintes termos: crítico(s); determinada; deve; é fundamental; é importante; é necessário; deve ser; devem; deverá; não deve; precisa ser; precisam; requer; tem, pode ser, é importante, essencial, é necessário e vital.

Quadro 3.1 – EVCR´s identificados na pesquisa bibliográfica

Fonte: autoria própria

EVCR´s À GOVERNANÇA DE TI	REFERÊNCIA	CONTEXTO
Comitês, Conselhos e Executivos de TI, papeis e responsabilidades	Definições claras e inequívocas dos papéis e responsabilidades das partes envolvidas são pré-requisitos críticos para um *framework* de governança eficaz de Tecnologia da Informação (ITGI, 2000), (Duffy, 2002).	Papéis e Responsabilidades de TI.
	O processo de Tomada de decisão em relação a governança de TI pode ser composto pela Unidade Dimensional Pessoas que incluem a arquitetura relacional dentro da organização, e os papéis e responsabilidades de diferentes *stakeholders* (Simonsson, 2006).	Tomada de Decisão.
	A eficácia da governança de TI é também determinada pela forma como a função de TI é organizada e onde a autoridade de tomada de decisão de TI está localizada dentro da organização (De Haes e Grembergen, 2004).	Posição da TI na organização.
	O CEO tem a responsabilidade singular para realização das políticas e planos estratégicos que foram estabelecidos pelo conselho e ele deve garantir que o diretor de TI seja parte do processo de decisão. O diretor de TI e o CEO devem reportar, regularmente ao conselho, que é o supervisor independente da conformidade e do desempenho do negócio (Duffy,2002).	Acompanhamento da TI pelo Conselho de Administração.
	O comitê estratégico de TI deve, evidentemente, trabalhar em estreita parceria com o Conselho, como também com outros comitês de gestão para orientar, rever e alterar o alinhamento empresarial das estratégias de TI e a implementação de estratégias de TI (De Haes e Grembergen, 2004).	Comitê Estratégico de TI. Comitê Executivo de TI.

EVCR´s À GOVERNANÇA DE TI	REFERÊNCIA	CONTEXTO
Alinhamento de TI/Modelos de Maturidade da governança.	Simonsson propõe um método para avaliação de maturidade da governança de TI dentro de uma empresa e, menciona que este tipo de avaliação é essencial para o bom acompanhamento, valorização e gestão das estruturas e processos de TI (Simonsson, 2008).	Tomada de Decisões Estratégicas e Monitoramento Estratégico da TI.
Aplicação de Melhores práticas de TI - *COBIT* e *ITIL*.	O domínio Planejar e Organizar (PO) do *COBIT* abrange 10 processos de TI estratégicos e táticos relativos à identificação da forma como a TI pode melhor contribuir para a consecução dos objetivos de negócios. A realização da visão estratégica precisa ser planejada, comunicada e gerenciada por diferentes perspectivas. Uma organização adequada, bem como infraestrutura tecnológica apropriada deve ser colocada em prática. (Simonsson, 2008).	Monitoramento Estratégico da TI.
***Balanced Scorecards* (TI)**	Segundo Kaplan R. e Norton D. (1992), as mensurações internas para o *balanced scorecard* devem partir de processos de negócios que têm o maior impacto nos fatores de satisfação do cliente que afetam o tempo, a qualidade, habilidade dos empregados e a produtividade. As empresas também devem tentar identificar e mensurar suas competências essenciais, as tecnologias críticas necessárias para garantir a liderança de mercado contínuo. As empresas devem decidir quais os processos e competências elas devem primar e especificar as medidas de cada um.	Tomada de Decisões Estratégicas e Monitoramento Estratégico da TI.
Cultural Organizacional	Uma organização que deseja implementar uma boa governança de TI deve ter uma cultura de apoio que suporte a governança. Isso significa que institucionalizar as boas práticas dos processos visando definir claramente os objetivos organizacionais e incentivar o *buy-in* para estes objetivos em todos os níveis (Norfolk, 2011).	Implementação da governança de TI.

EVCR´s À GOVERNANÇA DE TI	REFERÊNCIA	CONTEXTO
Desenvolvimento e Manutenção de Sistemas de Informação.	O desenvolvimento e a manutenção de sistemas automatizados devem ser firmemente baseados na análise e priorização de requisitos de negócios (incluindo requisitos regulamentares). Deve ser possível identificar por meio do negócio requisitos para código e vice-versa. O código deve contribuir para identificar objetivos de negócio (Norfolk, 2011).	Desenvolvimento e manutenção de sistemas.
Gestão de Acordos de Nível de Serviço.	Os principais desafios da governança é estabelecer que níveis de serviço devem ser expressos em termos de negócios, como também o lugar adequado do processo SLM / SLA (Haes e Grenbergen, 2004).	Monitoramento tático e operacional da TI.
	Em um ambiente de governança de TI maduro, o nível de serviço (SLAs) e seus processos de suporte ao gerenciamento de nível de serviço (SLM) precisam desempenhar um papel importante. De Haes e Grembergen (2004).	Tomada de Decisões Estratégicas e Monitoramento Estratégico da TI.
	O processo de Tomada de decisão em relação a governança de TI, pode ser composto pela Unidade Dimensional Processos, que incluem a implementação e a gestão de processos de TI, como por exemplo, o gerenciamento de nível de serviço (Simonsson, 2006).	Tomada de Decisão.
	O objetivo deste processo é documentar a celebração de acordos de nível de serviço (SLAs) entre os provedores e os consumidores de serviços de TI, e melhorar os níveis de serviço ao longo prazo, como as mudanças de negócios. Geralmente é importante que SLAs sejam orientados para o negócio (Norfolk, 2011).	Gestão de níveis de serviço.
	A que corresponde à capacidade / Nível de Maturidade 3, a governança de TI deve ter, pelo menos: Gestão de nível de serviço (Norfolk, 2011).	Processos necessários ao nível 3 de Maturidade da governança de TI.

EVCR´s À GOVERNANÇA DE TI	REFERÊNCIA	CONTEXTO
Gestão de Ativos	A que corresponde à capacidade / Nível de Maturidade 3, a governança de TI deve ter, pelo menos: Gestão de ativos locais, incluindo o gerenciamento de ativos de infraestrutura, de informação e de aplicação. (Norfolk, 2011).	Processo necessário ao nível 3 de Maturidade da governança de TI.
	Ter uma infraestrutura totalmente gerida com base atualizada e mantidos os registros dos ativos essenciais a governança de TI. Mesmo algo tão simples como a gestão de ativos é vital a governança de TI. (Norfolk, 2011).	Infraestrutura de ativos essenciais a governança.
	O processo de Tomada de decisão em relação a governança de TI pode ser composto pela Unidade Dimensional Tecnologia que representa as coisas físicas que as decisões consideram, como o *hardware* atual, os *softwares* e as instalações (Simonsson, 2006).	Tomada de Decisão
Gestão de Capacidade	A que corresponde à capacidade / Nível de Maturidade 3, a governança de TI deve ter, pelo menos: Planejamento de capacidade e provisionamento. (Norfolk, 2011).	Processo necessário ao nível 3 de Maturidade da governança de TI
	Deve haver um plano de capacidade, acordado com a administração e atribuído ao orçamento, de modo que possa ser implementado para assegurar que (em particular) possíveis faltas de capacidade não tenham impacto ao negócio (Norfolk, 2011).	Plano de Capacidade e de Continuidade do negócio.
Gestão de Configuração	A que corresponde à capacidade / Nível de Maturidade 3 a governança de TI deve ter, pelo menos: gerenciamento de configuração (Norfolk, 2011).	Processo necessário ao nível 3 de Maturidade da governança de TI
	A gestão de configuração fornece uma base para outros processos, como incidentes, problemas, alterações e Gestão de *Release*. Ela mantém um modelo lógico da infraestrutura de TI, armazenamento de CMDBs (bases de dados de gerenciamento de configuração) de forma federada e construídas a partir de "itens de configuração" (ICs). Gerenciamento de configuração é necessário, mas não suficiente para a efetiva governança de TI. (Norfolk, 2011).	Transição e Operação de Serviços.

EVCR´s À GOVERNANÇA DE TI	REFERÊNCIA	CONTEXTO
	O processo de Tomada de decisão em relação a governança de TI pode ser composto pela Unidade Dimensional Tecnologia que representa as coisas físicas que as decisões consideram, como o *hardware* atual, os *softwares* e as instalações. (Simonsson, 2006).	Tomada de Decisão.
Gestão de Continuidade de Negócios	A que corresponde à capacidade / Nível de Maturidade 3, a governança de TI deve ter, pelo menos a Implementação de uma política de continuidade de negócios (Norfolk, 2011).	Processo de Nível de Maturidade 3 à governança de TI
	Os planos de recuperação devem ser revistos regularmente para se certificar de que eles permanecem em alinhamento com as necessidades do negócio (Norfolk, 2011).	Planos de recuperação.
Gestão de Identidade	A que corresponde à capacidade / Nível de Maturidade 3, a governança de TI deve ter, pelo menos: Uma política de segurança em toda a organização, com base na gestão de riscos e gestão de identidade eficaz (Norfolk, 2011).	Processo necessário ao nível 3 de Maturidade da governança de TI.
Gestão de Incidentes	A que corresponde à capacidade / Nível de Maturidade 3, a governança de TI deve ter, pelo menos, gestão de incidentes (Norfolk, 2011).	Processo necessário ao nível 3 de Maturidade da governança de TI.
	O processo de Tomada de decisão em relação a governança de TI, pode ser composto pela Unidade Dimensional Processos, que incluem a implementação e a gestão de processos de TI, como por exemplo, o gerenciamento de incidentes (Simonsson, 2006).	Gestão de Processos de TI.
Gestão de Mudanças	Gestão de mudança não deve ser limitada ao ambiente real, embora as organizações muitas vezes dependam de processos de mudança de projeto para gerenciar mudanças em curso, em desenvolvimento, iniciativas, embora isso possa ser arriscado se a mudança para o ambiente de teste não é gerida, por exemplo, como ter a certeza de que o ambiente poderá validar as mudanças	Transição e Operação de Serviços.

EVCR´s À GOVERNANÇA DE TI	REFERÊNCIA	CONTEXTO
	correspondentes ao ambiente real, o que trará riscos consequentes para a entrega de serviços (Norfolk, 2011).	
Gestão de Problemas	A que corresponde à capacidade / Nível de Maturidade 3, a governança de TI deve ter, pelo menos: gestão de problemas (Norfolk, 2011).	Processo necessário ao nível 3 de Maturidade da governança de TI.
	Gerenciamento de problemas deve fornecer a organização com relatórios de informações relevantes de gestão (Norfolk, 2011).	Ações preventivas de Problemas/incidentes de TI.
Gestão de riscos	A que corresponde à capacidade / Nível de Maturidade 3, a governança de TI deve ter, pelo menos: uma política de segurança em toda a organização, com base na gestão de riscos e gestão de identidade eficaz (Norfolk ,2011).	Processo necessário ao nível 3 de Maturidade da governança de TI.
	A gestão da governança de TI e a boa segurança requer análise de riscos e ameaças, para determinar e priorizar os riscos enfrentados pela organização, e em seguida, a formulação de uma Política de Segurança, que documente as políticas destinadas a mitigar, transferir (por meio de seguros, por exemplo) ou aceitar (em conjunto com planos de contingência), os vários riscos identificados (Norfolk,2011).	Riscos de Segurança da informação.
Planejamento Estratégico de Sistemas de Informação.	O'Brien (2004) considera que um plano de SI deve evidenciar o custo-benefício esperado com a realização dos investimentos em SI bem como detalhes de todos os recursos materiais, humanos e tecnológicos para sua implementação. O plano de SI deverá permitir a visualização da viabilidade dos investimentos nos seguintes aspectos: – viabilidade organizacional: eficácia com que o sistema proposto apoia os objetivos estratégicos da organização; – viabilidade técnica: capacidade, confiabilidade e disponibilidade de hardware,	Planejamento de aquisição de soluções/serviços de TI. Tomada de Decisões Estratégicas e Monitoramento Estratégico da TI.

EVCR´s À GOVERNANÇA DE TI	REFERÊNCIA	CONTEXTO
	software e rede; – viabilidade econômica: economia de custo, aumento de receita, aumento de lucros; e – viabilidade operacional: aceitação por parte das pessoas que fazem a organização, apoio da alta gerência, atendimento a requisitos de clientes, fornecedores e governo.	
Política de Segurança da Informação	A que corresponde à capacidade / Nível de Maturidade 3, a governança de TI deve ter, pelo menos: uma política de segurança em toda a organização, com base na gestão de riscos e de gestão de identidade eficazes (Norfolk, 2011).	Processos necessários ao nível 3 de Maturidade da governança de TI.
	Segundo Norfolk (2011), um requisito para a boa governança de TI é a disponibilidade de uma política de segurança apropriada que deve ser mencionada no contrato de trabalho padrão do empregado e também fazer parte da sua formação inicial.	Segurança da informação.
Colaboração entre os principais stakeholders.	Peterson (2004), Figure 2 - *Structures, Processes and Mechanisms Relational for IT Governance.*	Participação de Stakeholder.
Entendimento compartilhado dos objetivos do negócio e da TI. (Gestão do Conhecimento)	Para De Haes e Grembergen (2004), assegurar o compartilhamento de conhecimento de forma contínua entre os departamentos e organizações é fundamental para atingir e manter o alinhamento entre o negócio e a TI.	Aprendizagem Compartilhada.
Localização (posição) do Negócio e da TI.	Peterson (2004), Figure 2 - *Structures, Processes and Mechanisms Relational for IT Governance.*	Parcerias Negócio e TI.
Negócio Multifuncional/Treinamento de TI (educação continuada e (*cross-training)*.	Peterson (2003), *Figure 2 - Structures, Processes and Mechanisms Relational for IT Governance.* Isto é crítico para facilitar o compartilhamento e a gestão do conhecimento por meio de mecanismos como educação continuada e treinamento *cross-training*, ou seja, que proporcionem a formação em diferentes tarefas ou habilidades.	Aprendizagem Compartilhada.

EVCR´s À GOVERNANÇA DE TI	REFERÊNCIA	CONTEXTO
Negócio Multifuncional/ Rotação de tarefas de TI. (profissionais *crossover)*	Peterson (2003), Figure 2 - *Structures, Processes and Mechanisms Relational for IT Governance.* Isto é crítico para facilitar o compartilhamento e a gestão do conhecimento por meio de mecanismos como profissionais *crossover* (equipes de TI trabalhando no negócio e equipes de negócios trabalhando na TI).	Aprendizagem Compartilhada.
Parcerias, recompensas e incentivos.	Peterson (2004), Figure 2 - *Structures, Processes and Mechanisms Relational for IT Governance.*	Parcerias Negócio e TI.
	Segundo Norfolk (2011), promover a governança de TI deve ser parte dos fatores de condição de trabalho do empregado com também a promoção de reconhecimento da boa governança em recompensas em prêmios e avaliação de pessoal.	Parcerias, recompensas e incentivos.
Participação ativa dos stakeholders principais	Peterson (2004), *Figure 2 - Structures, Processes and Mechanisms Relational for IT Governance*.	Participação de *Stakeholder*

3.2 – EVCR´s IDENTIFICADOS NA LEGISLAÇÃO

Foram identificados EVCR´s constantes da legislação aplicável, também às empresas públicas, abrangendo:

- Leis, Decretos, Instruções Normativas, e Normas Complementares da Presidência da República.

No escopo de análise foi considerada a Lei 13.303/2016, o Decreto 8.945/2016, a Instrução Nornativa Conjunta nª 01 MP/CGU, as Resoluções CGPAR e as Normas Complementares da Presidência da República.

É importante mencionar que desde 2008, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) tem realizado a publicação de normativos que visam disciplinar a gestão de segurança da informação e comunicações na Administração Pública Federal – APF, direta e indireta.

Encontra-se no Quadro 3.3 a lista desses normativos cuja leitura também busca expressões como “deve” ou “deverão” ou “deverá” ou “é vedado” ou “não devem”, dando origem aos EVCR´s já consolidados no Quadro 3.2. A lista das expressões referenciadas nos respectivos normativos encontra-se no Apêndice A.

Quadro 3.2 – EVCR´s identificados na Legislação Brasileira

EVCR´s À GOVERNANÇA DE TI IDENTIFICADOS NA LEGISLAÇÃO BRASILEIRA	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Comitês, Conselhos e Executivos de TI, papeis e responsabilidades	x	x	x	x		x	x
Alinhamento de TI/Modelos de Maturidade da governança.							
Aplicação de Melhores práticas de TI - *COBIT* e *ITIL*.							x
Avaliação de Desempenho - *Balanced Scorecards* (TI)			x				x
Cultural Organizacional	x						
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.			x		x	x	
Gestão de Acordos de Nível de Serviço.							x
Gestão de Ativos			x				x
Gestão de Capacidade			x				x
Gestão de Configuração			x				x
Gestão de Continuidade de Negócios			x				x
Gestão de Identidade							x
Gestão de Incidentes			x				
Gestão de Mudanças			x				
Gestão de Problemas			x				
Gestão de riscos	x	x	x	x	x		x
Planejamento Estratégico de Sistemas de Informação				x	x	x	
Política de Segurança da Informação				x			x
Colaboração entre os principais *stakeholders*							

EVCR´s À GOVERNANÇA DE TI IDENTIFICADOS NA LEGISLAÇÃO BRASILEIRA	1	2	3	4	5	6	7
Entendimento compartilhado dos objetivos do negócio e da TI. (Gestão do Conhecimento)							
Localização (posição) do Negócio e da TI							
Negócio Multifuncional/Treinamento de TI (educação continuada e (*cross-training).*							
Negócio Multifuncional/ Rotação de tarefas de TI. (profissionais *crossover)*							
Parcerias, recompensas e incentivos.							
Participação ativa dos *stakeholders* principais							

Fonte: autoria própria

1 – Lei 13.303/2016

2 – Decreto 8.945/2016

3 – Resoluções CGPAR

4 – Instrução Normativa Conjunta nº 01 – MP/CGU

5 - Instrução Normativa nº 2 da SLTI/MP

6 – Instrução Normativa nº 4 da SLTI/MP

7 – Normas Complementares da Presidência da República

Quadro 3.3 – Lista de Documentos Legais Avaliados

Fonte: autoria própria

Marcos Regulatórios	Finalidade	Publicação
Lei 13.303/2016	Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. Está Lei também é conhecida como "Lei das Estatais".	30 de junho de 2016.
Lei 6.404/1976	Dispõe sobre as Sociedades por Ações, também conhecida como Lei das SA´s.	15 de dezembro de 1976
Decreto 8.945/2016	Regulamenta, no âmbito da União, a Lei no 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.	27 de dezembro de 2016.
Instrução Normativa Conjunta MP/CGU Nº 01/2016	Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.	11 de maio de 2016.
Instrução Normativa n° 2, da SLTI/MP.	Dispõe sobre regras e diretrizes para a contratação de serviços, continuados ou não.	30 de abril de 2008.
Instrução Normativa n° 4, da SLTI/MP.	Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal	11 de setembro de 2014, alterada pela IN nº 2 de 12 de janeiro de 2015.
Resolução CGPAR nº-2, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações	Dispõe da adoção, pelas empresas estatais, de diretrizes objetivando o aprimoramento das suas práticas corporativas.	31 de dezembro de 2010.

Marcos Regulatórios	Finalidade	Publicação
Societárias da União – CGPAR.		
Resolução CGPAR nº-3, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR.	Dispõe da adoção, pelas empresas estatais, das diretrizes, objetivando o aprimoramento das práticas de governança corporativa, relativas ao Conselho de Administração.	31 de dezembro de 2010.
Resolução CGPAR Nº-11, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR.	Dispõe das empresas estatais que deverão planejar, implementar e manter práticas de governança de Tecnologia da Informação (TI) que atendam de forma adequada os padrões usualmente reconhecidos nesta área.	10 de maio de 2016.
Resolução CGPAR Nº-16, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR.	– A Resolução nº 16, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR, de 10 de maio de 2016, que dispõe das atribuições definidas na legislação societária e no estatuto social do Conselho de Administração das empresas estatais federais.	10 de maio de 2016.
Resolução CGPAR Nº-17, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR.	– A Resolução nº 17, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR, de 10 de maio de 2016, que dispõe das metas de desempenho empresarial vinculadas a planejamento estratégico.	10 de maio de 2016.
Resolução CGPAR Nº-18, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR.	– A Resolução nº 18, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR, de 10 de maio de 2016, que dispõe da implementação das políticas de Conformidade e Gerenciamento de Riscos.	10 de maio de 2016.
Resolução CGPAR Nº-20, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações	– A Resolução Nº 20, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR, de 17 de abril de 2017, que dispõe Trata das empresas estatais federais	17 de abril de 2017.

Marcos Regulatórios	Finalidade	Publicação
Societárias da União – CGPAR.	que deverão convocar Assembleia Geral para adaptação dos seus estatutos sociais à Lei nº 13.303, de 30 de junho de 2016 e ao Decreto nº 8.945, de 27 de dezembro de 2016.	
Norma Complementar - 02/IN01/DSIC/GSIPR	Definir a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta. "2.1 A metodologia de gestão de segurança da informação e comunicações baseia-se no processo de melhoria contínua, denominado ciclo **"PDCA"** *(Plan-Do-Check-Act)*, referenciado pela norma ABNT NBR ISO/IEC 27002:2006."	13 de outubro de 2008.
Norma Complementar – 03/IN01/DSIC/GSIPR	Estabelecer diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.	30 de junho de 2009.
Norma Complementar – 04/IN01/DSIC/GSIPR	Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.	14 de agosto de 2009.
Norma Complementar – 05/IN01/DSIC/GSIPR	Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.	14 de agosto de 2009.
Norma Complementar – 06/IN01/DSIC/GSIPR	Estabelecer diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.	11 de novembro de 2009.
Norma Complementar – 07/IN01/DSIC/GSIPR	Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.	06 de maio de 2010.
Norma Complementar – 08/IN01/DSIC/GSIPR	Disciplinar o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e	19 de agosto de 2010.

Marcos Regulatórios	Finalidade	Publicação
	indireta - APF.	
Norma Complementar – NC09/IN01/DSIC/GSIPR	Estabelecer orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta (APF).	19 de novembro de 2010.
Norma Complementar – 10/IN01/DSIC/GSIPR	Estabelecer diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.	30 de janeiro de 2012.
11/IN01/DSIC/GSIPR- Norma Complementar	Estabelecer diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.	30 de janeiro de 2012
Norma Complementar - 12/IN01/DSIC/GSIPR	Estabelecer diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	30 de janeiro de 2012.
Norma Complementar - 13/IN01/DSIC/GSIPR	Estabelecer diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).	30 de janeiro de 2012.
Norma Complementar -14/IN01/DSIC/GSIPR	Estabelecer diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	30 de janeiro de 2012.
Norma Complementar - 15/IN01/DSIC/GSIPR	Estabelecer diretrizes de Segurança da Informação e Comunicações para o uso das redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	30 de janeiro de 2012.

3.3 - EVCR´s IDENTIFICADOS EM ACÓRDÃOS DO TCU

O tema governança de TI na APF tem sido abordado de forma significativa por órgãos de fiscalização e controle, especialmente, o Tribunal de Contas da União, por meio da Secretaria de Fiscalização de Tecnologia da Informação – SEFTI, que desde o ano de 2007 tem realizado trabalhos de auditoria de TI, abordando os assuntos relacionados à governança de TI. Tais trabalhos resultaram na publicação de acórdãos, em que constam recomendações aos órgãos da APF (neste caso, inclui-se empresas públicas), a fim de tratar os fatores que impactam na governança de TI.

Segundo Meirelles (2005), a APF é assim caracterizada:

> O Estatuto da Reforma Administrativa (Dec-lei 200/67) classificou a Administração Federal em direta e indireta, constituindo a primeira "dos serviços integrados na estrutura administrativa da Presidência da República e dos Ministérios" (art. 4º, I), o que está ratificado, em outros termos, pelos arts. 15 e 29 da Lei 8.490/92. Quanto a indireta, apenas indica as categorias de entidades nela compreendidas, esclarecendo que são adotadas de personalidade jurídica própria e vinculadas ao Ministério em cuja área de competência se enquadrar sua principal atividade, gozando, entretanto, de autonomia administrativa e financeira (arts. 4º, II, e § 1º, e 5º, I a III, do Dec.-lei 200/67, a Administração indireta é a constituída dos serviços atribuídos a pessoas jurídicas diversas da União, Públicas (autarquias) ou privadas (empresas públicas e sociedades de economia mista), vinculadas a um Ministérios, mas administrativa e financeiramente autônomas.

As empresas públicas são pessoas jurídicas de direito privado, integrantes da Administração Indireta, instituídas pelo poder público, mediante autorização de lei específica, sob qualquer forma jurídica (Ltda, S/A etc.) e com capital exclusivamente público, para a exploração de atividades de natureza econômica ou execução de serviços públicos (ALEXANDRINO, 2006).

A criação de empresas públicas depende de lei específica autorizativa, nos termos do art. 37, XIX, da Constituição Federal (redação dada pela Emenda Constitucional

nº10/1998). São exemplos de empresas públicas: Empresa de Correios e Telégrafos - ECT; Caixa Econômica Federal - CEF, entre outras (ALEXANDRINO, 2006).

O respaldo legal aos órgãos de fiscalização e controle está previsto no artigo 70 da Constituição Federal em que consta o seguinte: a fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, à legitimidade, à economicidade, à aplicação das subvenções e à renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada poder.

Segundo o Artigo 71 da Constituição, o controle externo, a cargo do Congresso Nacional, será exercido com o auxílio do Tribunal de Contas da União, ao qual compete, dentre outras competências: julgar as contas dos administradores e demais responsáveis por dinheiros, bens e valores públicos da administração direta e indireta, incluídas as fundações e as sociedades instituídas e mantidas pelo poder público federal, e as contas daqueles que derem causa à perda, ao extravio ou à outra irregularidade de que resulte prejuízo ao erário.

Em análise dos acórdãos relativos à governança de TI, publicados pelo Tribunal de Contas da União, abrangendo o período de agosto de 2008 a novembro de 2014, citados no Quadro 3.4, foram obtidas informações acerca dos levantamentos e das recomendações relativas à governança de TI na APF.

Quadro 3.4 – Relação de acórdãos que tratam especificamente da governança de TI

Acórdão	Descrição	Publicação
Acórdão 3117/2014 Ata nº 45 – Plenário	Relatório de levantamento. Avaliação da governança de tecnologia da informação na Administração Pública Federal.	12/11/2014
Acórdão 2585/2012 Ata nº 38 – Plenário	Relatório de levantamento. Avaliação da governança de tecnologia da informação na Administração Pública Federal. Oportunidades de melhoria. Recomendações	26/09/2012
Acórdão 1233/2012 Ata nº 19 – Plenário	Gestão e uso de tecnologia da informação (TI). Relatório consolidado. 21 trabalhos, abrangendo 315 organizações públicas federais. Considerações a respeito das contratações de soluções de TI pelo sistema de registro de preços (SRP). Considerações sobre o tema "governança corporativa e governança de TI". Recomendações e determinações.	23/05/2012
Acórdão 1775/2012 Ata nº 26 – Plenário	Relatório de auditoria operacional em empresa pública. Tema de maior significância nº 7 de 2011 sobre sistemas informatizados de gestão das empresas estatais. Oportunidades de melhorias.	11/07/2012
Acórdão 1145/2011 Ata nº 15 – Plenário	Determinações e recomendações endereçadas a Órgãos de governança de TI na Administração Pública Federal. Avaliação do conjunto das medidas adotadas.	11/05/2011
Acórdão 2308/2010 Ata nº 33 – Plenário	Relatório de levantamento. Avaliação da governança de tecnologia da informação na Administração Pública Federal.	08/09/2010
Acórdão 1603/2008 Ata nº 32 – Plenário	Situação da governança de tecnologia da informação – TI na Administração Pública Federal. Ausência de Planejamento Estratégico Institucional. Deficiência na Estrutura de Pessoal. Tratamento inadequado à confidencialidade, à integridade e à disponibilidade das informações.	13/08/2008

Fonte: autoria própria

Em consulta realizada, via internet, ao sítio do Tribunal de Contas da União, no período de 02/04 a 07/06/2016, foi verificada a existência de 114 (cento e quatorze) acórdãos relacionados ao tema Tecnologia da Informação, aplicáveis também às empresas públicas, dentre estes foram selecionados os acórdãos citados a seguir, que tratam especificamente de levantamento acerca do tema Governança de TI no âmbito da APF, que são:

- Acórdão 1603/2008 – Ata 32 - TCU – Plenário – Brasil, publicado em 13/08/2008.

- Acórdão 2308/2010 – Ata 33 - TCU – Plenário – Brasil, publicado em 08/09/2010.

- Acórdão 1233/2012 – Ata 19 - TCU - Plenário – Brasil, publicado em 23/05/2012.

- Acórdão 2585/2012 – Ata 38 - TCU - Plenário – Brasil, publicado em 26/09/2012.

- Acórdão 3117/2014 – Ata 45 – TCU – Plenário – Brasil, publicado em 12/11/2014.

Em tais acórdãos procurou-se identificar EVCR´s, pela análise das ações e tratamentos relativos aos achados de auditoria em que constam os termos “deve” ou “devem” ou “não pode ser”, conforme Apêndice A1.

- Acerca do Acórdão nº 1603/2008 – TCU-Plenário, vale notar as seguintes observações:

  – O acórdão no 1603/2008 trata especificamente de levantamento da situação da governança de tecnologia da informação na Administração Pública Federal, tendo sido tala levantamento autorizado pelo acórdão 435/2007 - Plenário com o objetivo de “coletar informações acerca dos processos de aquisição de bens e serviços de TI, de segurança da informação, de gestão de recursos humanos de TI, e das principais

bases de dados e sistemas da Administração Pública Federal". Foram selecionados, como amostra, 333 órgãos/entidades representativos da Administração Pública Federal.

– Desses órgãos/entidades, 29 responderam em conjunto com outros órgãos/entidades e 14 não se consideram integrantes da Administração Pública Federal, apesar de jurisdicionados ao Tribunal, em especial os que fazem parte do sistema "S". Outros 25 órgãos/entidades não responderam à pesquisa e 10 não completaram a quantidade mínima estabelecida de respostas.

– Assim, 255 órgãos ou entidades participaram efetivamente do levantamento. Dessa relação constaram ministérios, universidades federais, tribunais federais, agências reguladoras, autarquias, secretarias, departamentos e empresas estatais. Ainda no planejamento, para ser submetido aos órgãos e às entidades da amostra, foi elaborado questionário composto de 39 perguntas baseadas nas normas técnicas brasileiras NBR ISO/IEC 17799:2005, NBR ISO/IEC 15999-1:2007 e no COBIT 4.1.

– Os achados mencionados no acórdão 1603/2008 estão relacionados às seguintes áreas da governança: planejamento estratégico institucional e de TI; estrutura de pessoal de TI; segurança da informação; gestão de acordos de níveis de serviço; processo de contratação de bens e serviços de TI; processo de gestão de contratos de TI; processo orçamentário de TI; auditoria de tecnologia da informação.

- Acerca do Acórdão 2308/2010 – TCU – Plenário, cabem as seguintes observações:

– O acórdão 2308/2010 trata do relatório de levantamento da avaliação da governança de tecnologia da informação na Administração Pública Federal, em cumprimento à determinação formulada pelo Acórdão 1603/2008 – TCU –

Plenário, pela qual a Secretaria de Fiscalização de Tecnologia da Informação realizou levantamento destinado a verificar a evolução, em relação à situação detectada em procedimento similar realizado em 2007, da governança de tecnologia da informação – TI no âmbito da Administração Pública Federal.

– Em 2007, o primeiro levantamento de governança de TI, com 39 questões e a participação de 255 instituições respondentes, resultou no Acórdão 1603/2008 – TCU, comentado acima. Naquela oportunidade, foram exaradas diversas recomendações estruturantes com vistas a fomentar a governança de TI na APF.

– A autorização para este levantamento consta no item 9.9 do referido acórdão, que determina à SEFTI a elaboração de outros levantamentos com o intuito de acompanhar e manter base de dados atualizada com a situação da governança de TI na Administração Pública Federal.

– Em análise ao acórdão 2308/2010, foi verificado que no teor do referido Acórdão são contemplados os achados citados no acórdão 1603/2008-TCU plenário.

Sendo assim, vale registrar os seguintes achados:

Achado I: dos órgãos/entidades pesquisados 57% não definiram objetivos de desempenho.

Achado II: dos órgãos/entidades pesquisados 76% não definiram indicadores de desempenho.

Achado III: Dos órgãos/entidades pesquisados 71% não avalia regularmente o desempenho.

Achado IV: dos órgãos/entidades pesquisados 87% não acompanha os indicadores de benefícios dos principais sistemas de informação.

Vale destacar que os dados encontrados, no referido levantamento, indicam que ao menos 57% dos respondentes não definiram objetivos de desempenho para o uso e para a gestão da TI institucional, sendo verificado que 76% não estabelecem indicadores de desempenho para TI, 71% não avaliam regularmente esse desempenho e 87% admitiram não tomar suas decisões quanto ao uso e à gestão de TI com base nos benefícios esperados dos sistemas de informação.

Portanto, a maioria das instituições respondentes não estabelece objetivos de TI, não tem indicadores de desempenho para esses objetivos, não avalia o alcance de objetivos e não toma decisões com base nos benefícios de negócios advindos dos sistemas de informação providos pela TI.

De forma geral, pode-se inferir que falta preocupação da alta administração com o uso e a gestão da TI institucional, o que pode induzir à ineficiência e não efetividade da instituição como um todo.

Assim, tendo em vista que esses aspectos estão na essência da governança, que se ampara na direção e no controle da gestão e do uso de TI, propõe recomendações a cada órgão governante superior para que:

- Oriente as instituições sob sua jurisdição, com base no princípio da eficiência, do planejamento e do controle, sobre a necessidade de a respectiva alta administração estabelecer formalmente:

- Objetivos institucionais de TI alinhados às estratégias de negócio.

- Indicadores para cada objetivo definido na forma acima, preferencialmente em termos de benefícios para o negócio da instituição.

- Metas para cada indicador definido na forma acima.

- Mecanismos que ela (alta administração) adotará para acompanhar o desempenho da TI da instituição.

- Promova, mediante orientação normativa, a obrigatoriedade de a alta administração de cada instituição sob sua jurisdição estabelecer os itens acima.

E finalmente, determinar que cabe à Sefti monitorar a APF quanto à evolução desses procedimentos.

Foi verificada, ainda, a realização de estudos a fim de avaliar a aderência dos órgãos/entidades da APF a governança de TI, com foco nas dimensões: liderança, estratégias e planos, pessoas e processos.

Os estudos foram realizados considerando a ponderação das subquestões do questionário dentro de uma questão, gerando um número que varia de 0 a 100% e que representa o grau de aderência da instituição à boa prática ou requisito legal em questão.

É importante mencionar que, para compor o índice de governança de TI (iGovTI), foram escolhidas somente as dimensões “1.liderança”, “2.estratégias e planos”, “6.pessoas” e “7.processos”, pois o aprofundamento do questionário nessas dimensões foi maior. Além disso, essas são as dimensões que, de uma forma ou de outra, foram abordadas no levantamento de 2007 (TCU-ACÓRDÃO 1603/2008).

Adicionalmente, a distribuição dos valores de iGovTI foi analisada em comparação com dois padrões de resposta ao questionário que, a juízo da equipe deste levantamento, representam a situação mais baixa que se possa classificar como governança intermediária e a situação mais baixa que se possa classificar como governança aprimorada. Esses dois padrões permitiram estabelecer os seguintes limites:

d) Abaixo de 40%, considera-se que a instituição se encontra em estágio inicial de governança de TI.

e) De 40 a 59%, considera-se em estágio intermediário.

c) A partir de 60%, considera-se em estágio aprimorado.

De acordo com as informações constantes do referido acórdão, pode-se observar que 57% das instituições respondentes se encontram abaixo do limite de 40% de aderência aos requisitos apresentados no questionário, o que corresponde ao estágio inicial de governança de TI.

Nessa faixa, o envolvimento da alta administração é menor, o planejamento mais frágil, os trabalhadores menos preparados e os controles internos são menos rigorosos e menos estruturados e, por isso, é maior o risco de ocorrência de falhas que costumam resultar em ineficácia, ineficiência, não efetividade e antieconomicidade.

Nas análises realizadas, foi verificado que dentre as organizações pesquisadas, 38% das instituições respondentes recaem no estágio intermediário de governança de TI.

Nessa faixa, há evidências de que a alta administração tem conhecimento de seu papel e que está preocupada em dar firme direção à instituição por meio de planejamento, reconhecendo a necessidade de pessoal qualificado para assumir processos e controles de processos mais rigorosos. Porém, tal condição ainda não se reflete consistentemente na formalização, monitoração e aperfeiçoamento de processos de trabalho, inclusive de planejamento, na fixação e monitoração de objetivos e no desenvolvimento sistemático do quadro de pessoal.

NA referida situação , o capital humano não está consolidado e a eventual troca da liderança poderá facilmente romper o processo de aperfeiçoamento institucional.

Resumindo, apenas 5% das instituições respondentes recaem no estágio aprimorado de governança de TI. Nesse estágio, encontram-se evidências do elevado compromisso da alta administração com a direção da instituição em todos os níveis, por meio de planejamento consistente e sistemático, fixação clara de objetivos e metas, monitoração da execução e auditoria. Além disso, o quadro de pessoal recebe qualificação sistemática e os processos de trabalho são formais e mensurados.

É importante citar que os estudos, ora apresentados, foram possivelmente realizados com base em informações de órgãos/entidades participantes de levantamento já realizado por meio do acórdão no 1603/2008 – TCU-plenário, visto que o acórdão 2308/2010, conforme já mencionado, trata-se de trabalho de acompanhamento e posicionamento das recomendações e encaminhamentos exarados no acórdão 1603/2008 – TCU-plenário.

- Acerca do Acórdão 2585/2012 – TCU – Plenário, cabem as seguintes observações:

O acórdão 2585/2012, publicado em 26/09/2012, trata de relatório de levantamento relativo a avaliação da governança de tecnologia da informação na Administração Pública Federal, com base no levantamento realizado no acórdão 2.308/2010-TCU-Plenário.

O acórdão 2505/2012, resultou no terceiro levantamento relativo à avaliação da Governança de TI na APF, realizado pelo TCU. O primeiro foi realizado em 2007 e contou com a participação de 255 instituições, resultando no acórdão 1603/2008 – TCU plenário.

O segundo levantamento, organizado em 2010, avaliou 301 instituições, dando origem ao acórdão 2308/2010 – TCU plenário, que apresentou, a evolução da situação de governança de TI na Administração Pública Federal - APF.

De acordo com as informações constantes dos acórdãos de nºs 1603/2008, 2308/2010 e 2585/2012 e a pesquisa realizada pelo TCU com base em uma amostra de 255 órgãos e entidades representativos da Administração Pública Federal, foi possível elaborar o quadro evolutivo da situação da governança de TI na Administração Pública Federal, conforme apresentado no Quadro 3.5 – consolidação de informações da APF, constantes em acórdãos do TCU.

- Acerca do Acórdão 3117/2014 – TCU – Plenário, cabem as seguintes observações:

O Acórdão 3117/2014, publicado em 12/11/2014, trata de relatório de levantamento relativo a avaliação da governança de tecnologia da informação na Administração Pública Federal, realizado a cada dois anos pelo Tribunal de Contas da União – TCU.

O presente trabalho foi conduzido pela Secretaria de Fiscalização de Tecnologia da Informação.

Com o objetivo de induzir a melhoria da governança de TI na APF, o TCU criou, um índice que busca refletir, de forma geral, a situação de governança de TI de cada organização avaliada, denominado de índice de governança de TI (iGovTI).

A partir de 2012, em atendimento ao Acórdão 2.308/2010-TCU-Plenário, a Sefti estabeleceu processo de trabalho para avaliar a governança de TI na APF em ciclos de dois anos.

No primeiro ano do ciclo, realiza-se a fase de coleta das informações por meio do levantamento de governança de TI. No ano seguinte, são realizadas auditorias específicas em uma amostra das organizações participantes, com o intuito de validar as respostas coletadas no levantamento, aprofundar a análise de alguns aspectos relacionados à governança e à gestão de TI e identificar boas práticas adotadas pelas organizações.

O Acórdão 3117/2014 abordou questões específicas sobre a governança de TI, por meio de três seções, que são:

- PERFIL DE GOVERNANÇA DE TI, apresenta a situação atual da Administração Pública Federal, bem como a evolução em relação ao ano de 2012;

- ÍNDICE DE GOVERNANÇA DE TI 2014 (iGovTI2014), são apresentados a definição e o método de cálculo desse índice, bem como os resultados consolidados da avaliação, com base nos números obtidos pelo iGovTI2014;

- PRINCIPAIS RISCOS E AÇÕES DE CONTROLE, em que são apresentados os níveis de risco associados às organizações, com base na relação entre iGovTI2014 e orçamento de TI aprovado em 2014.

Quadro 3.5 – Consolidação de informações da APF, constantes em acórdãos do TCU

Fonte: autoria própria

CONTEXTO	(Acórdão nº 1603/2008)	(Acórdão nº 2308/2010)	(Acórdão nº 2585/2012)	(Acórdão nº 3117/2014)
Planejamento estratégico institucional e de TI	Das organizações pesquisadas, 47% não têm planejamento estratégico institucional em vigor.	Das organizações pesquisadas, 80% possuem planejamento estratégico institucional em vigor.	Das organizações pesquisadas, 85% possuem planejamento estratégico institucional em vigor.	86% das organizações declaram executar processo de planejamento estratégico (item 'a'), sendo 66% de forma integral.
	Das organizações pesquisadas, 68% não possuem comitê diretivo de TI.	Das organizações pesquisadas, 50% não possuem comitê diretivo de TI.	Das organizações pesquisadas, 22% não possuem comitê diretivo de TI.	
		Das organizações pesquisadas, 67% possuem planejamento estratégico de TI.	Das organizações pesquisadas, 78% possuem planejamento estratégico de TI.	Das organizações pesquisadas, 75% declararam executar processo de planejamento de TI (17% parcialmente e 58% integralmente).
		Das organizações pesquisadas, 37% possuem plano diretor de TI.	Das organizações pesquisadas, 54% possuem plano diretor de TI.	77% das organizações declaram possuir plano de TI (PTI), (10% parcialmente e 67% integralmente).
Papéis e Responsabilidades				(52%) das organizações declarou avaliar a definição e compreensão de papéis e responsabilidades organizacionais (26% parcialmente e 26% integralmente).

CONTEXTO	(Acórdão nº 1603/2008)	(Acórdão nº 2308/2010)	(Acórdão nº 2585/2012)	(Acórdão nº 3117/2014)
				65% declararam dispor de código de ética, formalmente instituído, bem como divulgam e monitoram o seu cumprimento (23% parcialmente e 42% integralmente). A adoção desse normativo visa definir padrões de comportamento a serem seguidos pelos membros dos conselhos e da alta administração, bem como pelos gerentes da organização.
Documentação e Mapeamento de Processos críticos de negócio				66% das organizações declararam identificar e mapear os principais processos de negócio.
Estrutura de pessoal de TI	Das organizações pesquisadas, 5% afirmaram ter servidores que não são do quadro atuando na área de TI.	Das organizações pesquisadas, 6% afirmaram ter servidores que não são do quadro atuando na área de TI.		
		Das organizações pesquisadas, 64% das instituições preenchem as funções gerenciais de TI com pessoas do próprio quadro.	Das organizações pesquisadas, 73% das instituições preenchem as funções gerenciais de TI com pessoas do próprio quadro.	

CONTEXTO	(Acórdão nº 1603/2008)	(Acórdão nº 2308/2010)	(Acórdão nº 2585/2012)	(Acórdão nº 3117/2014)
	Das organizações pesquisadas 37% dos servidores que atuam nas áreas de TI não possuem formação específica em TI (incluindo aqui doutorado, mestrado, pós-graduação lato sensu e nível superior).	Das organizações pesquisadas 24% dos servidores que atuam nas áreas de TI não possuem formação específica em TI (incluindo aqui doutorado, mestrado, pós-graduação lato sensu e nível superior).		
	Das organizações pesquisadas 10% não possuem funções comissionadas voltadas à gestão de TI.	Das organizações pesquisadas 6% não possuem funções comissionadas voltadas à gestão de TI.		
	Das organizações pesquisadas 57% informaram que não possuem carreira específica para a área de TI.	Das organizações pesquisadas 21% informaram que não possuem carreira específica para a área de TI.		
		Das organizações pesquisadas 78% informaram ter carreira própria de TI..	Das organizações pesquisadas 77% informaram ter carreira própria de TI..	
		Das organizações pesquisadas 49% dependem de pessoal de TI externo à instituição.	Das organizações pesquisadas 40% dependem de pessoal de TI externo à instituição.	
Segurança da Informação	Das organizações pesquisadas, 34% possuem política de segurança da informação (PSI) formalmente definida.	Das organizações pesquisadas, 33% possuem política de segurança da informação (PSI) formalmente definida.	Das organizações pesquisadas, 45% possuem política de segurança da informação (PSI) formalmente definida.	

CONTEXTO	(Acórdão nº 1603/2008)	(Acórdão nº 2308/2010)	(Acórdão nº 2585/2012)	(Acórdão nº 3117/2014)
		Das organizações pesquisadas, 28% possuem inventário de ativos.	Das organizações pesquisadas, 24% possuem inventário de ativos.	
		Das organizações pesquisadas, 17% possuem gestão de configuração de ativos.	Das organizações pesquisadas, 30% possuem gestão de configuração de ativos.	
	Das organizações pesquisadas, 87% não possuem plano de continuidade de negócios (PCN).	Das organizações pesquisadas, 7% realizam Gestão da Continuidade dos serviços.	Das organizações pesquisadas, 17% realizam Gestão da Continuidade dos serviços.	Das organizações pesquisadas (27%) declararam dispor de política de gestão de continuidade do negócio formalmente instituída (19% parcialmente e apenas 8% integralmente).
	Ausência de gestão da capacidade e compatibilidade do ambiente de TI, em 84% dos órgãos/entidades pesquisados.	Das organizações pesquisadas, 6% possuem gestão da capacidade.	Das organizações pesquisadas, 15% possuem gestão da capacidade.	
	Das organizações pesquisadas, 22% possuem processo de classificação da informação.	Das organizações pesquisadas, 11% possuem processo de classificação da informação.	Das organizações pesquisadas, 17% possuem processo de classificação da informação.	
	Das organizações pesquisadas, 26% possuem processo de análise de riscos.	Das organizações pesquisadas, 17% possuem processo de análise de riscos.	Das organizações pesquisadas, 10% possuem processo de análise de riscos.	23% das organizações declararam dispor de política corporativa de gestão de riscos formalmente instituída (11% parcialmente e 12% integralmente)

CONTEXTO	(Acórdão nº 1603/2008)	(Acórdão nº 2308/2010)	(Acórdão nº 2585/2012)	(Acórdão nº 3117/2014)
	Dos órgãos/entidades pesquisados 48% declararam não possuir procedimentos de controle de acesso.			
	Dos órgãos/entidades pesquisados 88% dos pesquisados não realizam a gestão de mudanças.	Dos órgãos/entidades pesquisados 17% realizam gestão de mudanças.	Dos órgãos/entidades pesquisados 23% realizam gestão de mudanças.	
	Dos órgãos/entidades pesquisados 26% realizam a gestão de incidentes de Segurança da Informação.	Dos órgãos/entidades pesquisados 26% realizam a gestão de incidentes de Segurança da Informação.	Dos órgãos/entidades pesquisados 42% realizam a gestão de incidentes de Segurança da Informação.	
		Dos órgãos/entidades pesquisados 18% realizam gestão de problemas.	Dos órgãos/entidades pesquisados 28% realizam gestão de problemas.	
Desenvolvimento de sistemas de informação	Dos órgãos/entidades pesquisados 50% não adotam metodologia de desenvolvimento de *softwares*/sistemas.	Dos órgãos/entidades pesquisados 49% não adotam metodologia de desenvolvimento de *softwares*/sistemas.	Dos órgãos/entidades pesquisados 40% não adotam metodologia de desenvolvimento de *softwares*/sistemas.	
Gestão de acordos de nível de serviço	89% dos pesquisados informaram não executar a gestão de níveis de serviço de TI ofertados aos seus clientes.	Dos órgãos/entidades pesquisados 16% realizam gestão de nível de serviço.	Dos órgãos/entidades pesquisados 24% realizam gestão de nível de serviço.	

CONTEXTO	(Acórdão nº 1603/2008)	(Acórdão nº 2308/2010)	(Acórdão nº 2585/2012)	(Acórdão nº 3117/2014)
	73% dos pesquisados informaram que não executam a gestão de níveis de serviço dos serviços contratados, ou seja, mesmo quando o órgão/entidade é cliente e não fornecedor.	74% dos pesquisados informaram que não executam a gestão de níveis de serviço dos serviços contratados, ou seja, mesmo quando o órgão/entidade é cliente e não fornecedor.		
Processo de contratação de bens e serviços de TI	Das organizações pesquisadas 46% não adotam processo formal de trabalho para contratações de TI.	Das organizações pesquisadas 83% não adotam processo formal de trabalho para contratações de TI.		
	45% das organizações não realizam análise de viabilidade das contratações de TI.	48% das organizações não realizam análise de viabilidade das contratações de TI.		
	38% das organizações não explicitam os benefícios que a referida contratação pode gerar ao negócio.	58% das organizações não explicitam os benefícios que a referida contratação pode gerar ao negócio.		
Processo de gestão de contratos de TI	Das organizações pesquisadas, 53% não adotam processo formal de trabalho para gestão de contratos de TI.	Das organizações pesquisadas, 69% não adotam processo formal de trabalho para gestão de contratos de TI.		
		Das organizações pesquisadas, 14% adotam processo de planejamento das contratações de TI.	Das organizações pesquisadas, 18% adotam processo de planejamento das contratações de TI.	

CONTEXTO	(Acórdão nº 1603/2008)	(Acórdão nº 2308/2010)	(Acórdão nº 2585/2012)	(Acórdão nº 3117/2014)
	Das organizações pesquisadas 20% não designam formalmente um gestor para cada contrato de TI.	Das organizações pesquisadas 9% não designam formalmente um gestor para cada contrato de TI.		
	Das organizações pesquisadas 8% não realizam monitoração técnica dos contratos de TI.	Das organizações pesquisadas 3% não realizam monitoração técnica dos contratos de TI.		
	Das organizações pesquisadas 65% não realizam reuniões periódicas com os contratados para avaliar o desempenho de cada contrato de TI.			
	Das organizações pesquisadas 47% não definem previamente um critério para avaliação se as faturas apresentadas correspondem à realidade e se não contêm erros. (atestação técnica).			
	Em 55% das organizações pesquisadas a monitoração administrativa dos contratos de TI é realizada pela área de TI.			

CONTEXTO	(Acórdão nº 1603/2008)	(Acórdão nº 2308/2010)	(Acórdão nº 2585/2012)	(Acórdão nº 3117/2014)
	Em 57% das organizações pesquisadas não há transferência de conhecimento relativo aos produtos e serviços terceirizados para os servidores dos órgãos/entidades.			
Auditoria de tecnologia da informação	61% das organizações pesquisadas não realizaram Auditoria de TI nos últimos cinco anos.	54% das organizações pesquisadas não realizaram Auditoria de TI nos últimos 4 anos.	54% das organizações pesquisadas não realizaram Auditoria de TI nos últimos 4 anos.	
Governança de TI e a Alta Administração		47% das Organizações responsabilizam-se pelas políticas de TI.	54% das Organizações responsabilizam-se pelas políticas de TI.	
		50% das Organizações designaram Comitê de TI.	78% das Organizações designaram Comitê de TI.	76% dos participantes declararam dispor de um comitê de direção estratégica formalmente instituído
		37% das Organizações designaram Comitê de TI com representantes do negócio.	71% das Organizações designaram Comitê de TI com representantes do negócio.	
		21% das organizações monitoram o funcionamento do comitê de TI.	42% das organizações monitoram o funcionamento do comitê de TI.	
Desempenho Institucional na Gestão e uso da TI		43% definiram objetivos de desempenho.	54% definiram objetivos de desempenho.	

CONTEXTO	(Acórdão nº 1603/2008)	(Acórdão nº 2308/2010)	(Acórdão nº 2585/2012)	(Acórdão nº 3117/2014)
		24% definiram indicadores de desempenho.	37% definiram indicadores de desempenho.	
		71% das organizações não avaliam regularmente o desempenho da TI.		
		87% não acompanham os indicadores de benefícios dos principais sistemas de informação.		
		79% das organizações escolhem seus gestores de TI com base em suas competências.	85% das organizações escolhem seus gestores de TI com base em suas competências.	
Gestores de TI		Em 75% das organizações a alta administração não provê política de desenvolvimento de gestores de TI.		
		Em 83% das organizações a alta administração não acompanha o desempenho gerencial.		

3.4 – EVCR´s IDENTIFICADOS NAS MELHORES PRÁTICAS

Durante a identificação de EVCR´s à governança de TI em fontes de informação de órgãos reguladores e de governo, foi observada a referência à norma ISO/IEC 27002 e aos guias de melhores práticas de governança e de gestão de TI, como: o COBIT, o PMBOK, a ITIL, ocasionando, a necessidade de análise da relação destes elementos com aqueles identificados na pesquisa bibliográfica e em fontes de informação de órgãos reguladores.

Na referida análise foi considerada a versão 4.1 do COBIT, apesar da existência de versão mais recente, como o COBIT 5, com o propósito de assegurar a coerência às recomendações apontadas em acórdãos do TCU, considerando que nos acórdãos 1603/2008 e 2308/2010 é mencionado o COBIT 4.1. Os EVCR´s identificados constam do Quadro 3.6 e as análises realizadas constam do Apêndice B.

Quadro 3.6 – EVCR identificados nas melhores práticas e na Norma ISO 27002:2013

Fonte: autoria própria

EVCR´s	**1**	**2**	**3**	**4**	**5**
Planejamento Estratégico Institucional e de TI.	X	X			
Política de Segurança da Informação.	X		X		X
Papeis e Responsabilidades de TI.	X				X
Processo de Inventário e Mapeamento de Ativos.	X	X			X
Gestão de Continuidade de Negócios.	X	X			X
Classificação da Informação.	X	X			X
Controles de acesso relativos à Segurança da Informação e Comunicações.	X	X			X
Gestão de Riscos.	X		X	X	X
Gestão de Mudanças.	X	X			X
Gestão de Incidentes.	X	X			X
Processo de Desenvolvimento de Software.	X	X	X		X
Acordos de Níveis de Serviço.	X		X	X	X
Processo de Contratações de bens e serviços de TI.	X	X			X
Processo de Gestão de Contratos de TI.	X	X			X

EVCR´s	1	2	3	4	5
Gestão do Conhecimento.	X				X
Uso de Dispositivos Móveis.	X				X
Uso de computação em nuvem.					X
Participação de *Stakeholders.*	X				
Processo de Tomada de Decisão de TI.	X				
Treinamento e Capacitação em TI.	X				

Fonte: autoria própria

1 – COBIT

2 – ITIL

3 – PMBOK

4 – CMMI

5 – ISO 27002

3.5 – CONSOLIDAÇÃO DOS EVCR´s DE GOVERNANÇA DE TI

A partir do levantamento de EVCR´s, constantes na literatura acadêmica foi possível construir, de fato, a concepção dos EVCR´s associados à governança de TI.

Com base nos de EVCR´s associados à governança de TI identificados na literatura acadêmica, foi verificada também a existência destes nos Marcos Regulatórios que são: Leis, Decretos, Instruções Normativas, Normas Complementares, nos acórdãos do TCU, na norma ISO/IEC 27002:2013 e nos guias de melhores práticas, resultou na elaboração do Quadro 3.7.

Quadro 3.7 – Síntese dos EVCR´s associados à governança de TI

Fonte: autoria própria

EVCR´s	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Os conselhos e os executivos de TI e suas responsabilidades.	x	x	x	x						x
Os Colegiados de nível estratégico e tático.	x	x	x	x						
A representação da TI na alta liderança da organização.	x	x	x	x	x					x
A estrutura organizacional.	x	x	x	x						
Os papéis e Competências.	x	x	x	x				x	x	x
O Alinhamento da TI com os modelos de governança.	x									
A aplicação de melhores práticas de TI.	x								x	x
Metodologia de medição e gestão de desempenho – Balanced scorecards.	x									
A cultural organizacional.	x									
A aquisição, o desenvolvimento e a manutenção de soluções/serviços de TI	x	x	x			x	x	x	x	x
A gestão de acordos de nível de serviço.	x								x	x
A gestão de ativos.	x							x		x
A gestão de capacidade.	x									x
A gestão de configuração.	x							x		x
A gestão de continuidade de negócios.	x							x	x	x
A gestão de acesso físico e lógico.	x							x	x	x
A gestão de incidentes.	x							x		x
A gestão de mudanças.	x							x	x	x
A gestão de problemas.	x									x
A gestão de riscos.	x							x	x	x
O planejamento estratégico da TI.	x	x	x	x	x	x	x		x	x
A política de segurança da informação.	x			x				x	x	x
A colaboração e participação dos principais stakeholders.	x									
O entendimento compartilhado dos objetivos do negócio e da TI.	x									
A localização (posição) do negócio e da TI.	x									
O negócio multifuncional/treinamento de TI (educação continuada e treinamento cruzado (cross-training).	x	x	x		x			x	x	x
Gestão do Conhecimento	x	x	x		x			x	x	x

EVCR´s	1	2	3	4	5	6	7	8	9	10
O negócio multifuncional/ rotação de tarefas de TI (profissionais crossover).	x									
As parcerias, as recompensas e os incentivos.	x									

1 – Literatura Acadêmica
2 – Lei 13.303/2016
3 – Decreto 8.945/2016
4 – Resoluções CGPAR
5 – Instrução Normativa Conjunta nº 01 – MP/CGU
6 - Instrução Normativa nº 2 da SLTI/MP
7 – Instrução Normativa nº 4 – SLTI/MP
8 – Normas Complementares da Presidência da República
9 – Acórdãos do Tribunal de Contas da União que tratam do tema "governança de TI"
10 – Normas ISO/IEC e guias de melhores práticas em governança de TI

Após análise de EVCR´s, foi verificada a existência de similaridades nos EVCR´s da governança de TI identificados na pesquisa bibliográfica, com os EVCR´s identificados, na legislação brasileira, nas fontes de informação de órgãos reguladores e nas melhores práticas.

O objetivo deste capítulo foi demonstrar os EVCR´s selecionados na Literatura Acadêmica e, também o alinhamento destes com os Marcos Regulatórios, a norma NBR/ISO/IEC 27002:2013 e os guias de melhores práticas.

Após a seleção dos EVCR´s tornou-se necessária a validação destes numa organização, conforme descrito no capítulo 4.

4 – ESTUDO DE CASO – VALIDAÇÃO DOS EVCR´s

A análise foi realizada com o objetivo de verificar como uma empresa pública mantém a conformidade da governança de TI e como são tratadas, diariamente, as questões relativas a governança de TI, sendo aplicado como instrumento direcionador desta verificação os EVCR´s citados no Quadro 3.7.

O estudo de caso foi realizado em uma empresa pública, órgão da APF indireta. O negócio dessa organização é a prestação de serviços de TI para o governo federal, para tanto mantém um quadro de aproximadamente 10.0000 empregados, com Sede em Brasília.

Vale citar, ainda que a referida organização é pelos seguintes componentes estratégicos:

Visão: líder em soluções de tecnologia da informação e comunicações para realização das políticas públicas do governo federal.

Missão: Prover e integrar soluções em tecnologia da informação e comunicações para o êxito da gestão e da governança do Estado, em benefício da sociedade.

Premissas: conquistar reconhecimento de clientes, estado e sociedade; prestar serviços com pontualidade, inovação, qualidade e segurança; empregar soluções inovadoras com tecnologia adequada; desenvolver soluções de tecnologia da informação de forma cooperada; orientar a gestão para resultados que assegurem a sustentabilidade; praticar gestão integrada e participativa; manter os empregados comprometidos e motivados e atuar com ética e responsabilidade cidadã.

Negócio: tecnologia da informação e comunicações.

Produtos e serviços: sistemas de informação; serviços de tecnologia da informação e integração de soluções; consultoria e informações e gestão de TI dos sistemas estruturadores do Governo Federal.

Os levantamentos de dados contemplaram as informações relacionadas aos processos e os procedimentos de governança de TI aplicados na organização. Desta forma as fontes de dados e de informações foram: as políticas, as normas, a documentação de processos organizacionais relacionados a TI e os relatórios de verificação de conformidade da organização.

Diante da estratégia de pesquisa apresentada, foram identificadas as seguintes proposições de estudo:

a) Como as organizações públicas aplicam efetivamente os EVCR´s associados à governança de TI?

b) Que razões são motivadoras às organizações públicas para a aplicação de EVCR´s ?

Em relação às unidades de análise, de acordo com Yin (2001), a definição da unidade de análise está relacionada à maneira como as questões iniciais da pesquisa foram definidas. Sendo assim, as unidades de análise definidas neste trabalho, estão relacionadas aos EVCR´s associados à governança de TI, considerando os seguintes aspectos:

a) Verificar a aplicação de EVCR´s, em uma empresa pública.

b) Verificar, de forma qualitativa, o atendimento, por parte da organização aos EVCR´s.

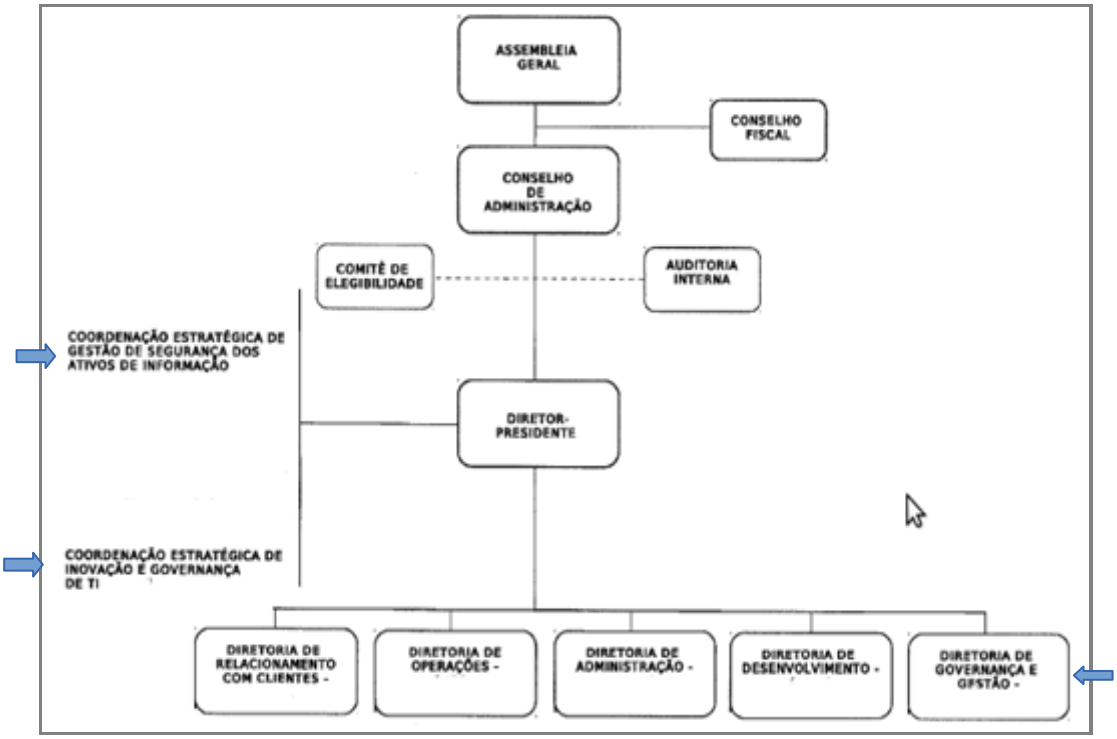
Os EVCR´s da governança de TI, identificados neste trabalho, demonstraram relação com questões relativas a Governança de TI, à Conformidade e à Segurança da

informação, motivando a realização do trabalho de análise nas Unidades organizacionais responsáveis por essas áreas de conhecimento.

As Unidades responsáveis pela Governança, Conformidade e Segurança da Informação estão subordinadas diretamente ao Diretor-Presidente da Empresa, e a área de conformidade está subordinada à Diretoria de Governança, conforme Figura 4.1.

Figura 4.1 – Organograma da organização

Fonte: autoria própria



O trabalho de análise foi aplicado com base na análise documental, sendo apoiado, também pela prática de reuniões com empregados das áreas relacionadas aos processos e as atividades da TI e, também com a realização de entrevistas com os responsáveis pelas áreas de Governança de TI, de Segurança da Informação e de Conformidade, conforme

destacado no organograma, como também a aplicação de verificação direta, apresentados no Quadro 4.2 – Validação dos EVCR`s.

Para realização da entrevista foi elaborado roteiro, constante do Apêndice 3, abrangendo em seu escopo as estruturas, os processos e os mecanismos de TI que compõe os EVCR´s.

Para aplicação de roteiro de entrevistas, inicialmente foram identificadas as áreas envolvidas e seus respectivos responsáveis, com base no documento de Descrição de atribuições e competências dessas áreas, especificamente as atividades relacionadas ao cumprimento de EVCR´s identificados na literatura acadêmica.

Com o objetivo de avaliar além o alinhamento e entendimento das práticas organizacionais na aplicação de EVCR´s, optou-se pela aplicação do mesmo modelo de roteiro de entrevista aos responsáveis pelas áreas envolvidas.

De acordo com a estrutura organizacional, segue a descrição das principais competências das áreas de Governança de TI, de Segurança da informação e de Conformidade, conforme apresentado no Quadro 4.1 - Competências das áreas responsáveis pela Governança de TI.

Quadro 4.1 - Competências das áreas responsáveis pela Governança de TI
Fonte: autoria própria

Resumo das Principais Competências das Áreas Responsáveis pelas Estruturas, Processos e Mecanismos de Governança de TI
Área Responsável pela Governança de Tecnologia da Informação
- Estruturar a Governança de Tecnologia da Informação. - Direcionar e coordenar os processos e as atividades relacionados à Governança de TI. - Elaborar e monitorar o Plano Estratégico de Tecnologia da Informação – PETI. - Elaborar e monitorar o Plano Diretor de Tecnologia da Informação – PDTI. - Promover o alinhamento das atividades de Governança de TI com Governança

Resumo das Principais Competências das Áreas Responsáveis pelas Estruturas, Processos e Mecanismos de Governança de TI
Corporativa. - Propor a melhoria continua das estruturas e processos relativos à Governança de TI. - Participar do Comitê Estratégico de TI.
Área Responsável pela Conformidade Institucional
- Direcionar e coordenar os processos e atividades relacionados à conformidade institucional. - Propor e acompanhar ações de conformidade institucional. - Apresentar relatório, periodicamente, das atividades de conformidade ao Conselho de Administração e à Diretoria Executiva. - Participar do Comitê Estratégico de TI.
Área responsável pela Segurança da Informação
- Participar de Comitês de Governança de TI, de Negócios e de Riscos, Conformidade e Segurança da Informação. – Interagir com as demais áreas da empresa, sempre que necessário, para adoção de ações inerentes às políticas e aos processos de Governança da Tecnologia da Informação. – Interagir com as áreas responsáveis pela educação corporativa, para apoio às ações educativas previstas pelos processos de Tecnologia da Informação. – Promover a estruturação da governança de TI por meio de ação conjunta com o comitê estratégico de segurança da informação. – Gerir os riscos dos processos de Governança de Tecnologia da Informação para estabelecer o equilíbrio entre as necessidades do negócio, bem como a adoção de controles adequados. – Promover a conformidade de Tecnologia visando assegurar o atendimento aos requisitos de segurança estabelecidos como resultado da necessidade do serviço, resultado de análise de riscos e classificação da informação. – Promover o fortalecimento da cultura de segurança da informação. – Estabelecer os conceitos, definir e implementar método de resiliência operacional nos processos da diretoria de operações. – Assegurar a conformidade dos processos, com foco na segurança da informação. – Realizar conformidade, periodicamente, nos processos de acordo com a cadeia de valor da organização. – Orientar, direcionar e prestar consultoria estratégica, tática e operacional às áreas que aplicam orientações de segurança da informação em seus processos, pessoas, procedimentos e atividades alinhando ao planejamento estratégico da organização. – Pesquisar e entender novas tendências e soluções tecnológicas focadas em segurança da informação, visando à elaboração de propostas de melhoria contínua dos processos de segurança da organização. – Colaborar de forma proativa às áreas que necessitem de apoio no tema segurança da informação.

No levantamento de informações da organização, foi possível observar que:

a) A organização tem como negócio a prestação de serviços de TI, o que torna os processos de governança de TI aplicáveis e necessários às atividades da organização.

b) A organização elegeu alguns serviços críticos, cujas ações de evolução e de melhoria contínua dos processos da TI são direcionadas, prioritariamente, para atendê-los.

c) A existência de uma diretoria para tratar as questões de conformidade e, também foi observado que área responsável pela verificação de conformidade, representa um ponto de controle aos processos organizacionais, pois são realizados trabalhos de verificação de conformidade, periodicamente, com foco nos processos corporativos, inclusive de TI, da organização.

As questões relatadas visam proporcionar um entendimento de como a governança de TI está estruturada dentro da organização. Acredita-se que após a verificação da aplicação dos EVCR´s associados à governança de TI, seja possível detalhar melhor a situação da governança de TI na organização.

No trabalho de análise documental, foram realizadas análises de documentos internos da organização, como: a cadeia de valor; o modelo de negócio; o modelo de governança de processos; o mapeamento e a documentação descritiva dos processos de: gestão de projetos; desenvolvimento de soluções; gestão integrada de serviços, segurança da informação; normativos internos da organização relacionados ao tema governança de TI, tecnologia da informação e segurança da informação; os normativos internos relativos à estrutura orgânica da organização; a relação de recomendações do TCU encaminhadas ao referido órgão, no período de 2008 a 2017; os documentos de atribuições e competência das áreas envolvidas com a governança de TI; os relatórios de verificação de conformidade

nos processos relacionados a governança de TI, tecnologia da informação e segurança da informação, no período de 2011 a 2017.

Com base nas informações obtidas por meio de análise documental, aplicação de entrevista e verificação direta, foi possível verificar a aplicação de elementos que orientam as ações de verificação de conformidade regulatória associados à governança de TI, em uma empresa pública, foi verificado o cumprimento dos EVCR´s citados no Quadro 3.7, conforme informações a seguir:

1. Os Conselhos e suas responsabilidades.

Foi verificada a existência de Conselho de Administração cujas responsabilidades constam do Estatuto Social da Organização e, também do Regimento Interno, inclusive, consta em documento organizacional normativo como competências do conselho de administração a aprovação do Plano Diretor de Tecnologia da Informação – PDTI e do Plano Estratégico de Tecnologia da informação – PETI alinhados ao Planejamento Estratégico da organização.

É importante mencionar que a criação de comitês estratégicos de TI e a elaboração do PETI e do PDTI estão previstas em marcos regulatórios, especificamente na Resolução CGPAR nº 11, as competências e responsabilidades do Conselho de Administração não são exaustivas em seu regimento interno, pois estas são complementadas, por meio do Estatuto Social da organização e documentos organizacionais internos.

2. Os Colegiados de TI e suas responsabilidades

De acordo com a entrevista realizada com os gestores responsáveis pelas áreas de Governança de TI e de Conformidade, o Colegiado de nível estratégico de Governança de Tecnologia da informação, é formado por Diretores Estatutários e empregados da organização das áreas de Governança, Riscos, Conformidade, Gestão de Pessoas e

Tecnologia da Informação, sendo que uma das competências deste Comitê e o acompanhamento da realização do PETI e do PDTI na organização.

Foi constatada, por meio de análise documental, a existência de documento normativo interno que institui este comitê e também formaliza as suas atribuições e competências.

A organização não estabeleceu colegiado de nível tático, até o momento, pois muitas questões a serem tratadas por este comitê são realizadas pelos gestores em processos específicos de tecnologia da informação, mas de acordo como as determinações constantes do artigo 2º, inciso V da Resolução CGPAR nº 11 é necessário instituir comitê tático.

3. A representação da TI na alta liderança da organização

A liderança de TI é parte do Colegiado Estratégico de Tecnologia da Informação e, também da Diretoria Executiva da organização membro da diretoria responsável pela Tecnologia da Informação. A Diretoria executiva tem como competência analisar e aprovar por meio do processo decisório da organização as proposições do diretor de tecnologia da informação, ou seja as decisões estratégicas de tecnologia da informação são proposta pelo Diretor de Operações são deliberadas em colegiado pela Diretoria Executiva da Organização.

4. A estrutura organizacional da Empresa

De acordo com o organograma, citado na figura 4.1, a estrutura organizacional é representada da seguinte forma:

- Assembleia Geral
- Conselho de Administração

- Conselho Fiscal
- Auditoria Interna
- Diretoria Executiva
- Colegiados em nível estratégico
- Diretoria de Relacionamento com Clientes
- Diretoria de Desenvolvimento de Software
- Diretoria de Governança
- Diretoria de Operações

É importante citar que esta estrutura organizacional além de atender uma estrutura de Governança de TI, está em conformidade com as determinações da Lei 6.404/76, da Lei 13.303/2016 e do Decreto 8.945/2016 e também com o Estatuto Social da organização.

A Diretoria de Operações é responsável pela elaboração da maioria das proposições relacionadas à tecnologia da informação, votadas e aprovadas em processo decisório, pela diretoria executiva.

De acordo com a estrutura organizacional a auditoria interna tem o papel e a competência de assessorar o conselho de administração. Tal situação guarda conformidade com os marcos regulatórios, especificamente a Lei 13.303/2016 e o Decreto 8.945/2016.

Sendo verificado ainda que a estrutura da diretoria de governança foi criada em 2016, para tratar dos assuntos de governança de forma corporativa na organização, visando também fortalecer os mecanismos de governança, riscos, conformidade, integridade e controles internos conforme determina a Instrução Normativa Conjunta nº 01 do MP/CGU.

5. Os papéis e Competências dos Membros Estatutários e empregados da organização

As competências dos membros estatutários que compõe o Conselho de Administração e a Diretoria Executiva estão previstos no Estatuto Social da empresa,

porém essas competências não são exaustivas há também o regimento interno do Conselho e os documentos organizacionais diretivos que tratam também de outras competências não previstas no Estatuto Social da Organização.

As competências dos empregados estão formalizadas por meio documento e são estabelecidas de acordo com área em que o empregado está lotado estando também relacionadas à área de especialização deste.

As competências dos Membros Estatutários guardam conformidade com a Lei 13.303/2016, com o Decreto 8.945/2016 e com as Resoluções CGPAR nºs 02, 03 e 16.

6. O Alinhamento da TI com os modelos de governança

A organização trabalha com alguns modelos de governança, sendo a governança de processos, a governança corporativa e a governança de tecnologia da informação.

O alinhamento da TI com estes modelos de governança ocorre da seguinte forma:

- Os processos de TI são mapeados seguindo o modelo de governança de processos da organização;

- A governança corporativa aponta em alguns momentos para a governança de TI. A organização trata de forma separada, ou seja, equipes trabalham governança corporativa e outras equipes trabalham governança de TI, havendo integrações e compartilhamento de informações entre as equipes.

– A Governança de TI é um modelo em construção e a organização está trabalhando na estruturação de modelo padronizado de governança, há um grupo de trabalho voltado para o FACIN que é um framework de governança aplicável à administração pública federal, há também ações que direcionam para aplicação de controles do Cobit e do COSO como uma opção para estruturação da Governança, não sendo possível evidenciar a existência de direcionamento formalizado da organização quanto a essa busca de padrões.

7. A aplicação de melhores práticas de TI

A organização aplica melhores práticas de TI, de acordo com os relatórios de avaliação de conformidade, foi possível constatar a aplicação das seguintes melhores práticas:

– PMBOK, no gerenciamento de projetos relacionados ao planejamento estratégico da organização e dos projetos de TI que estão relacionados aos objetivos estratégicos da organização.

– CMMI nos processos, procedimentos e artefatos relacionados ao macro processo de desenvolvimento e de manutenção de software da organização.

– COSO nos processos de governança, de gestão de riscos e de conformidade.

– ITIL na gestão do ciclo de vida dos serviços de TI da organização.

– Cobit nos processos de governança e de gestão da tecnologia da informação e de segurança da informação.

– Aplicação de normas ISO relacionadas a gestão de riscos, a segurança da informação, continuidade de negócios e conformidade.

– Aplicação de metodologia para avaliação de conformidade dos processos da organização baseada no Manual de Auditoria Operacional do Tribunal de Contas da União – TCU.

8. Metodologia de medição e gestão de desempenho – Balanced scorecards

Foi constatado que a organização aplica *balanced scorecards* na gestão de desempenho de processos estratégicos, não sendo evidenciada a aplicação deste nos processos de TI.

9. Fomentação da Cultural Organizacional

A cultura organizacional é fomentada por meio dos seguintes mecanismos:

a) Estabelecimento de comitês interdisciplinares em nível estratégico;

b) Realização de seminários abordando temos críticos da organização relacionados a tecnologia da informação e de interação das áreas de conformidade, riscos e controles internos com as demais áreas da organização, com base na aplicação de procedimentos formalizados e reuniões técnicas.

10. Processo de desenvolvimento e de manutenção de Tecnologias

A organização tem processo específico de aquisição de tecnologias baseado no regulamento de licitações e contratos estabelecido na Lei 13.303/2016 e no Decreto 8.945/2016, dentre outras legislações pertinentes.

O processo de aquisição e de manutenção de tecnologias é baseado na melhor prática *Capability Maturity Model Integration* – CMMI, que é um modelo integrado de capacidade e de maturidade. Há também soluções de TI que suportam este processo na produção de artefatos.

É importante citar que os requisitos de segurança previstos na Norma Complementar nº 16, são considerados nas atividades deste processo.

11. Processo de aquisição e de contratação de Produtos e Serviços

A organização tem processo formalizado para a aquisição de tecnologias e, também o regulamento de licitações e contratos estabelecido na Lei 13.303/2016 e no Decreto 8.945/2016.

É importante mencionar que em análise as recomendações do Tribunal de Contas da União – TCU, direcionadas à Organização, por meio do Relatório de Gestão de 2016, foram emitidas recomendações relacionadas a necessidade de melhorias no processo de aquisição e de contratações da organização, especificamente da fase de planejamento deste.

De acordo com os apontamentos do TCU, a organização necessita aprimorar seus processos visando cumprir, nas fases de aquisição e de gestão, o que foi efetivamente planejado.

12. A gestão de acordos de nível de serviço

A gestão de acordos de nível de serviço é realizada pelos gestores, ou seja cada contrato de despesa tem um gestor administrativo e o gestor técnico para supervisionar as atividades de gestão dos contratos.

A área responsável pelo monitoramento da disponibilidade dos serviços gera insumos aos gestores técnicos do cumprimento dos acordos de nível serviços.

13. A gestão de ativos

O processo de gestão de ativos está muito focado na gestão do serviço sendo realizado com o apoio de tecnologias.

Em análise aos relatórios de avaliação de conformidade, produzidos pela área de conformidade em segurança da informação da organização, foi verificado que organização precisa aprimorar sua base de gestão de configuração de ativos (CMDB).

14. A gestão de capacidade

O processo de capacidade da organização é mais tangível nas atividades voltadas para a plataforma alta (mainframe), em consulta aos relatórios de avaliação de conformidade nos ambientes de plataforma avançada, foi verificada a necessidade de aprimoramento do processo de gestão de capacidade da plataforma avançada.

15. A gestão de configuração

O processo de gestão de configuração está voltado para as questões de gestão de serviços, ou seja, a gestão e a manutenção da configuração tem como base as demandas da gestão de serviços, por exemplo, os itens de configuração são verificados periodicamente e de forma minuciosa quando há algum indicio de incidente ou de mudanças.

É importante mencionar que a gestão de configuração é realizada com o apoio de tecnologias.

16. A gestão de continuidade de negócios

O processo de gestão de continuidade está formalizado e está estruturado por meio de comitês e gestores de continuidade.

Os gestores de continuidade são empregados da organização responsáveis pelas atividades de conformidade.

Os planos de continuidade são elaborados, inicialmente, para os sistemas e serviços considerados críticos pela organização.

Este segmento é tratado pela área de segurança da informação da organização, sendo verificado que há estruturas e normas internas específicas que tratam deste assunto, inclusive, os referidos normativos referenciam a necessidade de cumprimento às determinações da Norma Completar nº 06 da Presidência da Republica, que estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

17. Gestão de Acesso físico

Foi verificada a existência de processo de acesso físico e também de normativo que trata deste assunto.

A organização aplica níveis de segurança diversificados aos vários ambientes da organização, que são:

a) Áreas de acesso crítico ou sensível: áreas e estruturas específicas de elevado grau de controle e registros de acesso. Hospedam informações, equipamentos e dispositivos que suportam processos de negócio da organização ou de seus clientes;

b) Áreas de acesso restritas ou estratégicas: áreas que são caracterizadas por armazenar e manipular informações da organização cujo grau de acesso seja "restrito";

c) Áreas de risco: áreas com elevado grau de risco à vida humana e que hospedem recursos básicos para manutenção e continuidade dos serviços e ambientes;

d) Áreas de uso corporativo: áreas que não hospedam informações, dispositivos ou atividades de caráter restrito. Ambientes comuns de convivência e circulação de pessoas.

Com base nestas definições são estipuladas as regras de acesso a cada área da organização.

Há também controles físicos implementados, como: disponibilização de catracas em pontos estratégicos de acesso, identificação e registro em sistema para acesso as dependências internas da organização, uso de crachá com mecanismo biométrico.

Nos ambientes de acesso restrito são aplicados os mecanismos já citados e, também outros como: porta eclusa, câmeras, monitoramento contínuo.

18. Gestão de Acesso lógico

Há sistema de controle de acesso de usuários em que os estes são bloqueados automaticamente quando estão em férias ou de licença e as chefias são notificadas via e-mail corporativo.

O acesso às estações de trabalho pelos empregados é realizado via *token*, assegurando assim o não repudio.

19. A gestão de incidentes

Foi verificada a existência de processo de gestão de incidentes cujas atividades estão formalizadas e são realizadas com base na ITIL.

Sendo verificada também a existência de documentos normativos internos que mencionam a obrigatoriedade de atendimento à Norma Complementar nº 08, do Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República do Brasil, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

20. A gestão de mudanças

Foi verificada a existência de processo de gestão de mudanças cuja as atividades estão formalizadas e são realizadas com base na ITIL.

Sendo verificada também a existência de documentos normativos internos que mencionam a obrigatoriedade de atendimento a Norma Complementar nº 13/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República do Brasil, estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta.

21. A gestão de problemas

Foi verificada a existência de processo de gestão de problemas cujas atividades estão formalizadas e realizadas com base na ITIL.

Sendo verificada também a existência de documentos normativos internos que mencionam a obrigatoriedade de atendimento à Norma Complementar nº 08, do Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República do Brasil, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal, pois de acordo com o entendimento da organização a gestão de problemas está diretamente relacionada a gestão de incidentes.

22. A gestão de riscos

A gestão de riscos está baseada em dois componentes principais: Política e metodologia, sendo que os conceitos e determinações da política de riscos tem como referência as determinações da Instrução Normativa conjunta MP/CGU Nº 01.

A metodologia de riscos estão baseada na norma ABNT NBR ISO 31000 – Gestão de riscos: princípios e diretrizes; na NBR ISO 31004 Gestão de Riscos – Guia para Implementação da ABNT ISO 31000 e no *Committee of Sponsoring Organizations* – COSO.

Foi verificada também a existência de Política de Gestão de Riscos alinhada às determinações constantes da Resolução nº 18, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR, de 10 de maio de 2016, que dispõe da implementação das políticas de Conformidade e Gerenciamento de Riscos.

Em entrevista com o gestor responsável pela área de riscos e de conformidade, foi constado que não há solução de TI que atenda de forma eficaz a automação dos processos e procedimentos aplicados na gestão de riscos da organização. Atualmente a organização está trabalhando na prospecção de soluções para este fim.

23. Planejamento Estratégico

O planejamento estratégico é elaborado, com base na matriz de *Swot*, a partir dessa análise os objetivos estratégicos são definidos e estes são acompanhados pela alta liderança e pelos gestores por meio de tecnologias de gestão de projetos. O planejamento é definido considerando o plano de negócios e a estratégia de longo prazo, com análise de riscos e oportunidades para os próximos 5 (cinco) anos, conforme determina o artigo 23 da Lei 13.303/2016.

As atividades de planejamento estratégico também consideram as determinações da Resolução nº 17, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR, de 10 de maio de 2016, que dispõe das metas de desempenho empresarial vinculadas a planejamento estratégico.

Na aplicação de análise documental e, também em entrevista com os gestores da área de Governança de TI e de Conformidade, foi mencionado o alinhamento do Planejamento estratégico da organização, com o Planejamento Estratégico da TI – PETI e o Plano Diretor de Tecnologia da Informação – PDTI.

O alinhamento ocorre por meio da definição de objetivos estratégicos do Planejamento Estratégico que apontam para os projetos e ações de Tecnologia da Informação, propostas no PETI e no PDTI da organização.

24. A política de segurança da informação

A política de segurança da informação da organização está formalizada e abrange os aspectos de segurança informações em relação a continuidade de serviços, acesso físico e lógico, a cultura de segurança da informação, desenvolvimento de softwares, monitoramento dos sistemas e serviços e conformidade.

Sendo verificada também a existência de documentos normativos internos que mencionam a obrigatoriedade de atendimento à Norma Complementar nº 03/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República do Brasil, que dispõe de Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

25. A colaboração e participação dos principais stakeholders

Foi constatada a participação dos principais *stakeholders* na elaboração de propostas do planejamento estratégico da organização.

Sendo verificado também que organização promove reuniões técnicas e eventos com a participação de Clientes.

26. O entendimento compartilhado dos objetivos do negócio e da TI

O entendimento compartilhado dos objetivos do negócio e da Tecnologia da Informação envolve também a cultura organizacional, sendo necessária a participação de representantes da TI nos comitês estratégicos de Negócios da organização e a partir desta ação, as decisões são tratadas nos níveis tático e operacional.

Em entrevista realizada com o responsáveis pelas áreas de Governança de TI e de Segurança de TI foi citado que estes participam do Comitê de Negócios da Organização.

Cabe citar ainda a existência de proposta para análise de macro processos organizacionais, a fim de promover melhor integração entre os processos de negócios e de Tecnologia da Informação.

27. A localização (posição) do negócio e da TI

O negócio ocupa uma posição privilegiada na organização, pois é responsável por internalizar as demandas.

Em entrevista com o gestor responsável pela área de Governança de Tecnologia da Informação, foi mencionado que a área de Tecnologia da Informação participa das negociações após a avaliação de viabilidade por parte da área de negócios, ou seja área de

TI tem a prerrogativa de influenciar e direcionar a área de negócios por meio de soluções inovadoras.

28. O negócio multifuncional/treinamento de TI (educação continuada e treinamento cruzado - *cross-training*, Gestão do Conhecimento)

Foi constatada a existência de área que trata dos treinamentos de empregados, a maioria destes são promovidos via Educação a Distância – EAD, nestes treinamentos são abordados temas variados negócios, tecnologia da informação entre outros, há também grades de treinamento específicas e obrigatórias aos gestores que são pré-requisitos para promoção por mérito.

O corpo funcional, não gestores, também possuem grade de treinamento, são realizadas também palestras direcionadas aos gestores e ao corpo funcional da organização.

A organização também investe em certificações na área de TI para seus empregados, dentre as certificações obtidas, podemos destacar: ITIL, COBIT, CMMI, PMBOK, ISO 27001, entre outras.

29. O negócio multifuncional/ rotação de tarefas de TI (profissionais crossover)

Em entrevista com o gestor da área de Tecnologia da informação, este afirmou que a organização tem propostas para promover profissionais *crossover*, mas não foi colocada em prática.

Sendo possível verificar que a organização possui áreas com conhecimento multidisciplinar o que pode promover o negócio multifuncional e a gestão do conhecimento, considerando que empregados com especializações distintas trabalharão juntos, compartilhando conhecimento. Não sendo possível evidenciar a aplicação de mecanismos que promovam a rotação de tarefas.

30. Gestão do Conhecimento

Foi verificado que a gestão do conhecimento é tratada de por meio de mecanismos de compartilhamento de informações, como ambientes de colaboração, há também mecanismos de comunicação entre os empregados e gestores, por exemplo, os empregados sugerem propostas para o planejamento estratégico da organização e realizam suas proposições por meio destes mecanismos.

31. As parcerias, as recompensas e os incentivos

Foi constatada a existência de promoção por mérito como mecanismos de recompensa aos empregados.

Após aplicação de entrevistas com os gestores responsáveis pela área de conformidade e de riscos e conformidade e a aplicação de análise documental e em alguns casos verificação direta, foi possível verificar a situação do cumprimento de EVCR´s associados à governança de TI na organização, considerando as situações “atendido”, “ parcialmente atendido”, conforme Tabela 4.2.

Quadro 4.2 - Validação de EVC`s

Fonte: autoria própria

Descrição do EVCR´s	Situação	Justificativa	Método de verificação
1. Os Conselhos e suas responsabilidades.	Atendido	Os Conselhos estão instituídos na estrutura organizacional e suas responsabilidades formalizadas.	Análise documental e entrevista.
2. Os Colegiados de TI e suas responsabilidades.	Atendido Parcialmente	Não instituído o comitê tático de TI, conforme determina o artigo 2º, inciso V da Resolução CGPAR nº 11.	Análise documental e entrevista.

Descrição do EVCR´s	Situação	Justificativa	Método de verificação
3. A representação da TI na alta liderança da organização	Atendido	A TI está representada na Diretoria Executiva da organização, por meio da Diretoria de Operações e também a área responsável pela Governança de TI está subordinada ao Diretor-Presidente. As decisões estratégicas de tecnologia da informação são proposta pelo Diretor de Operações e deliberadas em colegiado pela Diretoria Executiva da Organização.	Análise documental e entrevista.
4. A estrutura organizacional da Empresa	Atendido	A estrutura organizacional além de atender a estrutura de Governança de TI, está em conformidade com as determinações da Lei 6.404/76, da Lei 13.303/2016 e do Decreto 8.945/2016 e também com o Estatuto Social da organização.	Análise documental.
5. Os papéis e Competências dos Membros Estatutários e empregados da organização.	Atendido	As competências dos empregados estão formalizadas por meio documento e são estabelecidas de acordo com área em que o empregado está lotado estando também relacionadas a área de especialização deste.	Análise documental.
6. O Alinhamento da TI com os modelos de governança.	Atendido Parcialmente	A Governança de TI é um modelo em construção e a organização está trabalhando na estruturação de modelo padronizado de governança, A governança corporativa aponta em alguns momentos para a governança de TI.	Análise documental.
7. A aplicação de melhores práticas de TI.	Atendido	A organização aplica melhores práticas de TI, de acordo com os relatórios de avaliação de conformidade, foi possível constatar a aplicação das melhores nos processos de TI da organização.	Análise documental e entrevista.
8. Metodologia de medição e gestão de desempenho – Balanced scorecards	Atendido Parcialmente	Foi constatado que a organização aplica *balanced scorecards* na gestão de desempenho de processos estratégicos, não sendo evidenciada a aplicação deste nos processos de TI.	Análise documental e entrevista.
9. Cultural Organizacional	Atendido	A organização apresentou a aplicação de ações que visam fomentar a cultura organizacional.	Análise documental e entrevista.
10. Processo de	Atendido	O processo de aquisição e de	Análise

Descrição do EVCR´s	Situação	Justificativa	Método de verificação
desenvolvimento e de manutenção de Tecnologias.		manutenção de tecnologias está baseado na melhor prática Capability Maturity Model Integration – CMMI, que é um modelo integrado de capacidade e de maturidade. Há também soluções de TI que suportam este processo na produção de artefatos. É importante citar que os requisitos de segurança previstos na Norma Complementar nº 16, são considerados nas atividades deste processo.	documental e entrevista.
11. Processo de aquisição e de contratação de Produtos e Serviços.	Atendido Parcialmente	O processo está em fase de revisão e melhorias, conforme Relatório de Gestão de 2016, o Tribunal de Contas da União – TCU, emitiu recomendações relacionadas a necessidade de melhorias no processo de aquisição e de contratações da organização, no que tange a fase de planejamento deste.	Análise Documental.
12. A gestão de acordos de nível de serviço.	Atendido	A gestão de acordos de nível de serviço é realizada por gestores, ou seja cada contrato de despesa tem um gestor administrativo e o gestor técnico para supervisionar as atividades de gestão dos contratos.	Análise Documental.
13. A gestão de ativos	Atendido Parcialmente	Em análise aos relatórios de avaliação de conformidade, produzidos pela área de conformidade em segurança da informação da organização, foi verificado que organização precisa aprimorar sua base de gestão de configuração de ativos (CMDB).	Análise Documental.
14. A gestão de capacidade.	Atendido Parcialmente	Necessidade de aprimoramento do processo de gestão de capacidade da plataforma avançada.	Análise Documental.
15. A gestão de configuração	Atendido	O processo de gestão de configuração está voltado para as questões de gestão de serviço, ou seja, a gestão e manutenção da configuração é impulsionada pela gestão de serviços.	Análise Documental.
16. A gestão de	Atendido	O processo de gestão de continuidade	Análise

Descrição do EVCR´s	Situação	Justificativa	Método de verificação
continuidade de negócios		está formalizado e está estruturado por meio de Comitês e gestores de continuidade e considera em seus processos as determinações da Norma Complementar nº 06 da Presidência da República.	Documental.
17. A gestão de acesso físico	Atendido.	Os requisitos de acesso físico estão implementados, estando formalizada a obrigatoriedade de atendimento à Norma Complementar nº 07 que estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	Análise Documental e verificação direta.
18. Gestão de Acesso lógico	Atendido.	Os requisitos de acesso lógico estão implementados, estando formalizada a obrigatoriedade de atendimento à Norma Complementar nº 07 que estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	Análise Documental e verificação direta.
19. A gestão de incidentes	Atendido.	As atividades de gestão de incidentes estão formalizadas e realizadas com base na ITIL. Sendo verificada também a existência de documentos normativos internos que mencionam a obrigatoriedade de atendimento à Norma Complementar nº 08, do Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República.	Análise Documental.
20. A gestão de mudanças	Atendido.	Foi verificada a existência de processo de gestão de mudanças cuja as atividades estão formalizadas e são	Análise Documental.

Descrição do EVCR´s	Situação	Justificativa	Método de verificação
		realizadas com base na ITIL. Sendo verificada também a existência de documentos normativos internos que mencionam a obrigatoriedade de atendimento a Norma Complementar nº 13/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República.	
21. A gestão de problemas	Atendido.	Foi verificada a existência de processo de gestão de problemas cuja as atividades estão formalizadas e são realizadas com base na ITIL.	
22. A gestão de riscos	Atendido Parcialmente.	Em entrevista com o gestor responsável pela área de riscos e de conformidade, foi constado que não há solução de TI aplicada na gestão de riscos da organização. Atualmente a organização está trabalhando na prospecção de soluções de TI para este fim.	
23. Planejamento Estratégico	Atendido.	Na aplicação de análise documental e, também em entrevista com os gestores da área de Governança de TI e de Conformidade, ambos citaram o alinhamento do Planejamento estratégico da organização, com o Planejamento Estratégico da TI – PETI e o Plano Diretor de Tecnologia da Informação – PDTI da organização.	Análise documental e entrevista.
24. A política de segurança da informação	Atendido.	A política de segurança da informação da organização está formalizada e abrange os aspectos de segurança informações em relação a continuidade de serviços, acesso físico e lógico, a cultura de segurança da informação, desenvolvimento de softwares, monitoramento dos sistemas e serviços e conformidade.	Análise documental.
25. A colaboração e participação dos principais stakeholders	Atendido.	Foi constatada a participação dos principais stakeholders na elaboração de propostas do planejamento	Análise documental e entrevista.

Descrição do EVCR´s	Situação	Justificativa	Método de verificação
		estratégico da organização.	
26. O entendimento compartilhado dos objetivos do negócio e da TI.	Atendido.	O entendimento compartilhado dos objetivos do negócio e da Tecnologia da Informação envolve também a cultura organizacional, sendo necessária a participação de representantes da TI nos comitês estratégicos de Negócios da organização e a partir desta ação, as decisões são tratadas nos níveis tático e operacional.	Análise documental e entrevista.
27. A localização (posição) do negócio e da TI	Atendido.	O negócio ocupa uma posição privilegiada na organização, sendo assim a área de negócios é responsável pela internalização das demandas, a área de Tecnologia da Informação participa das negociações após a avaliação de viabilidade por parte da área de negócios, ou seja área de TI tem a prerrogativa de influenciar e direcionar a área de negócios por meio de soluções inovadoras.	
28. O negócio multifuncional/treinamento de TI (educação continuada e treinamento cruzado - cross-training, Gestão do Conhecimento)	Atendido.	Foi constatada a existência de área que trata dos treinamentos de empregados, a maioria destes são promovidos via Educação a Distância – EAD, nestes treinamento são abordados temas variados negócios, tecnologia da informação entre outros, há também grades de treinamento específicas e obrigatórias aos gestores que são pré-requisitos para promoção por mérito.	Análise documental e entrevista.
29. O negócio multifuncional/ rotação de tarefas de TI (profissionais crossover)	Atendido Parcialmente.	Em entrevista com o gestor da área de Tecnologia da informação, este afirmou que a organização tem propostas para promover profissionais *crossover*, mas ainda não foi colocada em prática.	Análise documental e entrevista.
30. Gestão do Conhecimento	Atendido.	Foi verificado que a gestão do conhecimento é tratada de por meio de mecanismos de compartilhamento de informações, como ambientes de colaboração, há também mecanismos de comunicação entre os empregados e	Análise documental e entrevista.

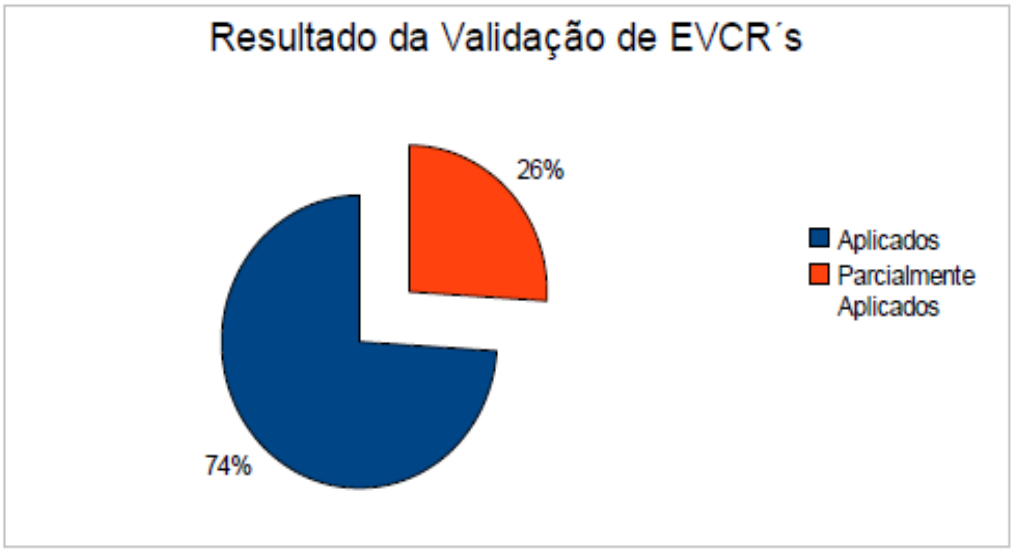
Descrição do EVCR´s	Situação	Justificativa	Método de verificação
		gestores, por exemplo, os empregados sugerem propostas para o planejamento estratégico da organização e votam por meio destes mecanismos.	
31. As parcerias, as recompensas e os incentivos	Atendido.	Foi constatada a existência de promoção por mérito como mecanismos de recompensa aos empregados.	Análise documental.

Fonte: autoria própria

Desta forma foi possível verificar que 74% dos EVCR´s associados a governança de TI são aplicados, 26% são parcialmente aplicados, conforme Figura 4.2.

Figura 4.2 - Aplicação de EVCR´s à governança de TI

Fonte: autoria própria



Diante das informações e das evidências apresentadas pela organização, foi possível observar que o cumprimento aos EVCR´s da governança de TI está, fortemente, relacionado às recomendações e as orientações governamentais procedentes do Tribunal de Contas da União, do Ministério do Planejamento, Desenvolvimento e Gestão e da Presidência da República.

Os resultados das análises identificaram similaridades, conforme apresentado no Quadro 4.3.

Quadro4.3 - Análise da aplicação de EVCR´s associados à governança de TI – similares

Fonte: autoria própria

Referências	**EVCR´s- similares**
Pesquisa bibliográfica; informações de órgãos reguladores; Marcos Regulatórios e melhores práticas.	Os conselhos e os executivos de TI e suas responsabilidades.
	Os Colegiados de nível estratégico e tático.
	A representação da TI na alta liderança da organização.
	A estrutura organizacional.
	Os papéis e Competências.
	O desenvolvimento, a aquisição e a manutenção de Tecnologias.
	O planejamento estratégico.
	A gestão de riscos.
	O negócio multifuncional.

Sendo verificada similaridade em 29% dos EVCR´s.

Foi constatado que em 32% dos elementos que orientam ações de verificação de conformidade regulatória associados a governança de TI representam os EVCR´s identificados na pesquisa bibliográfica, conforme demonstrado no Quadro 4.4.

Quadro4.4 - Análise da aplicação de EVCR´s associados à governança de TI – Exclusivos
Fonte: autoria própira

Literatura Acadêmica	**EVCR´s – exclusivos**
	O Alinhamento da TI com os modelos de governança.
	Metodologia de medição e gestão de desempenho – *Balanced scorecards.*
	A Cultural organizacional.
	A colaboração e participação dos principais *stakeholders.*
	O entendimento compartilhado dos objetivos do negócio e da TI.
	A colaboração participação entre os principais *stakeholders*.
	O entendimento compartilhado dos objetivos do negócio e da TI.
	A localização (posição) do negócio e da TI.
	O negócio multifuncional, a rotação de tarefas da TI. (Profissionais *crossover)*
	As parcerias, as recompensas e os incentivos.

Quanto a análise de EVCR´s e o processo de tomada de decisão da organização, foi verificado na análise documental que as ações estratégicas da organização, como aquisições e projetos de tecnologia da informação são encaminhados à alta liderança, no caso à Diretoria executiva, por meio de proposições do Diretor de Operações que apresenta a referida proposta para deliberação e aprovação da Diretoria Executiva da Organização.

Foi verificado que os relatórios gerados pela área de conformidade são encaminhados às áreas envolvidas e às diretorias da organização, sendo observado que as recomendações constantes dos referidos relatórios possuem desdobramentos relevantes aos processos de tomada de decisão da organização, considerando que:

– As recomendações podem ser inseridas no planejamento estratégico da organização, contribuindo desta forma com o correlato processo de tomada de decisão.

– As recomendações podem ser parte de planos de ações abordando os níveis estratégico, tático e operacional da organização.

– As recomendações podem ser incluídas em um processo de acompanhamento, realizado pela área de conformidade, até que as não conformidades sejam devidamente tratadas.

Foi verificado que o processo de conformidade institucional desempenha um papel importante no direcionamento dos processos da TI, pois as ações deste processo abrangem, também, a conformidade dos EVCR´s, ocasionando benefícios ao processo de tomada de decisão da organização, sendo verificado ainda que a metodologia aplicada neste processo está prevista no Manual de Auditoria Operacional do Tribunal de Contas da União - TCU.

5 – CONCLUSÕES E RECOMENDAÇÕES

Este trabalho se propôs a identificar EVCR´s associados à governança de TI, com base na pesquisa bibliográfica, nos Marcos Regulatórios e nas orientações e recomendações de órgãos reguladores, na norma ISO/IEC 27002:2013 e nos guias de melhores práticas de governança e de gestão de TI.

O presente trabalho, inicialmente buscou definições relativas à governança de TI e, também na identificação de Estruturas, Processos e Mecanismos de TI cuja consolidação ocasionou a identificação de EVCR´s associados à governança de TI baseados na pesquisa bibliográfica.

Sendo verificado que as definições de Governança de TI, se diferenciem em alguns aspectos, em virtude do próprio período em que foram escritas e, abordam, fortemente, as questões relacionadas à tomada de decisão, considerando: o nível de autoridade de decisão da TI na organização (estrutura), o modo com que os recursos de TI são gerenciados e controlados (processos e mecanismos), buscando sempre alinhar os investimentos às estratégias corporativas da TI.

Os estudos realizados identificaram EVCR´s associados à governança de TI, apresentados no Quadro 3.7 – Síntese dos EVCR´s associados à governança de TI que podem apoiar as ações de verificação de conformidade regulatória em organizações públicas. Desta forma, a pesquisa atendeu ao seu objetivo proposto inicialmente que é identificar EVCR´s à governança de TI.

Complementarmente, o estudo se propôs a investigar e verificar a aplicabilidade de EVCR´s associados a governança de TI em um órgão da Administração Pública Federal brasileira, por meio da aplicação de análise documental, aplicação de entrevistas e de verificação direta.

De acordo com as análises realizadas, foi verificado que os EVCR´s, procedentes de órgãos de fiscalização e controle e da legislação tem prioridade no cumprimento pela organização, principalmente aqueles relacionados aos acórdãos do TCU.

Desta forma, foi possível constatar que a aplicação efetiva de EVCR´s direciona e aprimora as ações de governança de TI e, promove o cumprimento aos dispositivos legais e às recomendações de órgãos de fiscalização e controle.

Observou-se que a aplicação dos EVCR´s está vinculada ao processo corporativo denominado "verificar conformidade", assegurando, desta forma, a aplicação da conformidade regulatória e a melhoria contínua dos processos organizacionais.

Foi verificado que nos relatórios gerados pela área de conformidade constam recomendações direcionadas à melhoria dos processos de Governança de TI e também de outros processos organizacionais, como o processo de tomada de decisão da organização.

É importante mencionar que as não conformidades e as recomendações mais críticas, assim como relatórios das atividades de conformidade são apresentadas, periodicamente, aos Conselhos de Administração e Fiscal e à Diretoria Executiva.

Sendo constatado que o processo "verificar conformidade" desempenha um papel importante no direcionamento dos processos da TI, pois o escopo de conformidade institucional da organização abrange, também, a conformidade dos EVCR´s, ocasionando o fortalecimento das práticas de Governança de TI na organização.

Os resultados apresentados possibilitam concluir que os EVCR´s associados à governança de TI identificados neste trabalho, abrangem as práticas de governança de TI aplicadas, internamente, na organização.

Com base na verificação da aplicação de EVCR´s associados à governança de TI, em uma empresa pública, foi verificado que a governança de TI, está em processo de

evolução, considerando a necessidade de tratamento as questões críticas relacionadas aos seguintes assuntos:

a) definição da metodologia da estrutura de governança de TI;

b) o aprimoramento de tecnologias que atendam efetivamente a gestão de riscos;

c) o tratamento de questões operacionais que podem impactam fortemente nos processos de negócios, como a necessidade de aprimoramento da base de ativos de informação da organização; e

d) por fim a implementação de mecanismos que possibilitem a capacitação de profissionais com conhecimento integrado das atividades de TI e do negócios da organização, denominados na literatura acadêmica, como profissionais *crossover*, estes apontamentos podem impactar, fortemente, na evolução e funcionamento da governança de TI.

Quanto à realização de trabalhos futuros, foi observado que os EVCR´s associados à governança de TI podem ser aplicados como orientadores às estruturas, processos e mecanismos de Governança de TI, assim como instrumento de consulta na elaboração de trabalhos relativos a verificação de conformidade regulatória a governança de TI nas organizações públicas brasileiras.

ARTIGOS PUBLICADOS

Clara, C. M. A; Junior, .S.T. R; Canedo, E. Actions to verify compliance of a public company with IT Governance. 12th Iberian Conference on Information Systems and Technologies (CISTI). Lisbon, Portugal, June 2017. IEEE. DOI: 10.23919/CISTI.2017.7975834. http://ieeexplore.ieee.org/abstract/document/7975834/?reload=true.

Clara, C. M. A; Junior, S.T. R; Canedo, E. Elements that Orient the Regulatory Compliance Verification Audits on ICT Governance dg.o '17. Staten Island, NY, USA, June 2017. ACM. table of contents ISBN: 978-1-4503-5317-5 doi>10.1145/3085228.3085286. https://dl.acm.org/citation.cfm?id=3085286

Clara, C. M. A; Junior, S.T. R; Canedo, E. Elementos que orientam ações de conformidade regulatória à Governança de TI. CONTECSI - International Conference on Information Systems and Technology Management, Universidade de São Paulo – USP, São Paulo, SP, Maio 2017. ISSN 2448-104.

REFERÊNCIAS BIBLIOGRÁFICAS

Alexandrino, M., Paulo V., Direito administrativo. Rio de Janeiro, Brasil. Impetus, 2006.

Bloem, J.; Van Doorn, M.; Mittal, P. Making IT governance work in a Sarbanes-Oxley world. New Jersey: John Wiley & Sons, 2006.

De Haes, S.; Grembergen, W.V; IT governance and its mechanisms. Informations Systems Control Journal, volume 1, 2004.

Duffy J., 2002, IT/business alignment: Is it an option or is it mandatory?, IDC document, nr. 26831.

Duffy J., 2002, IT governance and business value part 1, IDC document, nr. 27291.

Eisenhardt, K.M. (1989). "Building Theories from Case Study Research". In The Academy of Management Review, Vol. 14, No. 4. (Oct., 1989), pp. 532-550.

Gil, A. C. (2010). Como Elaborar Projetos de Pesquisa. 5ª Edição. Editora Atlas. São Paulo.

Grembergen, W. V; De Haes, S.; Guldentops, E. Structures, processes and relational mechanisms for IT governance. Idea Group Publishing, 2004.

Grembergen, W. V.; Strategies for information technology governance. Idea Group Publishing, 2004.

Hamaker, S., Hutton, A: Principles of IT governance. Information Systems Control Journal, Volume 2, 2004.

Hardy, G. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. Information Security technical report, 2006.

Henderson, J.C.; Venkatraman, N. Strategic alignment: a model for organizational transformation via information technology. Center for Information Systems Research, Sloan School of Management, Massachusetts Institute of Technology, 1990.

Henderson, J.C.; Venkatraman, N. Strategic alignment: leveraging information technology for transforming organizations. IBM System Journal, v. 38, 1999.

Larsen, H. M.,Pedersen K. M., and Andersen, V. K. IT governance – Review 17 IT Governance tools and analyzing the Case of Novozymes A/S. In Proceedings of the 39th Hawaii International Conference on System Sciences. Hawaii, January 2006. IEEE. DOI http://doi.ieeecomputersociety.org/10.1109/HICSS.2006.234.

IBGC. Instituto Brasileiro de Governança Corporativa, http://www.ibgc.org.br/Secao.aspx?CodSecao=17, acessado em 07/01/2013.

IT Governance Institute - ITGI, COBIT 4.1., ISBN 1-933284-72-2. USA, pp. 8.

IT Governance Institute - ITGI: Board briefing on IT governance. Available online at www.itgi.org, 2000.

IT Governance Institute - ITGI. *Board briefing on IT*. IT Governance Institute, 2ª ed., 2003.

IT Governance Institute – ITGI. Control Objectives for Information and Related Technology, 4th Edition 2005. http://www.itgi.org.

IT Governance Institute - ITGI. Aligning COBIT 4.1, ITIL V3, ISO/IEC 27002 for Business Benefit - A Management Briefing From ITGI and OGC, 2008.

Kaplan R, Norton D., *The balanced scorecard – measures that drive performance*, Harvard Business Review, January-February, 1992.

Korac-kakabadse, N.; Kakabadse, A. IS/IT governance: need for an integrated model. Corporate Governance, v. 1, n. 4, 2001.

Lagerström, R.: Modifiability and usability. Dissertação de Mestrado. Department of Industrial Information and Control Systems, Royal Institute of Technology, KTH, Stockholm, Sweden 2005.

Lunardi, G.; Dolci, P.; Becker, J; Maçada, A.; Governança de TI no Brasil : uma análise dos mecanismos mais difundidos entre as empresas nacionais. Universidade Federal do Rio Grande do Sul - UFRGS - Repositório Digital, 2007. Disponível em http://www.lume.ufrgs.br/handle/10183/31080?locale=en.

Luftman, J. Competing in the Information age – Strategic alignment in Practice. Oxford University Press, 1996.

Meirelles, L. H. Direito Administrativo Brasileiro. São Paulo, Brasil. Malheiros, 2005.

Norfolk, D.IT Governance. Thorogood Pub. Limited, 2011.

Object Management Group. Business Process Model and Notation (BPMN), OMG Document Number: formal/2009-01-03, pp. 1, 2008.

O' Brien, J.A. Sistemas de informação e as decisões gerenciais na era da Internet 2ª ed. São Paulo: Saraiva, 2004.

Parker M. Strategic transformation and information technology. Prentice Hall, Upper Saddle River (NJ), 1996.

Peterson, R. Crafting information technology governance. Information Systems Management, 2004.

Peterson, R. Integration strategies and tactics for information technology governance. In: VAN GREMBERGEN, W. Strategies for information technology governance, Hershey: Idea group publishing, 2004.

PMI – Project Management Institute. Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos (Guia PMBOK®) 3ª edição. 2004.

PMI - Project Management Institute. Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos (Guia PMBOK®) 4ª edição, 2008.

Proctor, P. E, Compliance Key Initiative Overview. Gartner, 2011. ID: G00214765. Disponível em https://www.gartner.com, acessado em 14/01/2014.

Ribbers, P. M. A; Peterson, R. R. Parker, M.M. Designing information technology governance processes: Diagnosing contemporary practices and competing theories. Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.

Ridley, G., Young, J., Carroll, P. COBIT and its utilization: A framework from the literature. Proceedings of the 37th Hawaii International Conference on System Sciences, 2004.

Sambamurthy, V.; Zmud, R. Arrangements for information technology governance: a theory of multiple contingencies. MIS Quarterly, v. 23, n. 2, 1997.

Santos, L.A.A; Lemes, S. A lei Sarbanes_Oxley: uma tentativa de recuperar a credibilidade do mercado de capitais norte-americano. São Paulo. FEA/USP, 2004.

Schramm, W. Notes on case studies of instructional mediaprojects.Working paper, the Academy for Educational Development, Washington, DC, 1971.

SEI - Software Engineering Institute. CMMI - Capability Maturity Model Integration - CMMI for Development, Version 1.3 - Carnegie Mellon University, 2010.

SEI - Software Engineering Institute. CMMI - Capability Maturity Model Integration - CMMI for Development, Version 1.2 - Carnegie Mellon University, 2006.

Silveira, A. Governança corporativa, desempenho e valor da empresa no Brasil. São Simonsson, M., and Johnson, P., Defining IT Governance - A Consolidation of Literature. Working Paper of the Department of Industrial Information and Control Systems., 2006a.Availible online at www.ics.kth.se.

Simonsson, M., Predicting IT Governance Performance: a method for model-based decision making, 2008.

Simonsson, M., Johnson, P., "Defining IT Governance - A Consolidation of Literature. Working Paper of the Department of Industrial Information and Control Systems, 2006.

Simonsson, M., Ekstedt, M., Getting the Priorities Right - Literature versus Practice on IT Governance. Accepted for publication at Portland International Conference on Management of Engineering and Technology, Istanbul, July 9-13, 2006.

Sohal, A.S., Fitzpatrick, P.: IT Governance and Management in Large Australian Organization. International Journal of Production Economics. Elsevier Science, 2002.

Tribunal de Contas da União – Acórdão 1603/2008 – Ata 32 – TCU – Plenário – Brasil, publicado em 13/08/2008.

Tribunal de Contas da União – Acórdão 2308/2010 – Ata 33 – TCU – Plenário – Brasil, publicado em 08/09/2010.

Tribunal de Contas da União – Acórdão 1233/2012 – Ata 19 – TCU – Plenário – Brasil, publicado em 23/05/2012.

Tribunal de Contas da União – Acórdão 2585/2012 – Ata 38 – TCU – Plenário – Brasil, publicado em 26/09/2012.

Turban, E.; Mclean, E.; Wetherbe, J. Tecnologia da informação para gestão. Porto Alegre: Bookman, 3ª ed., 2004.

Van der Heijden, H.: Measuring IT Core Capabilities for Electronic Commerce - Results From a Confirmatory Case Study. Proceedings of the twenty first international conference on information systems, 2000.

Van Grembergen, W.: Introduction to the minitrack IT governance and its mechanisms. Proceedings of the 35th Hawaii International Conference on System Sciences. IEEE, 2002.

Van Grembergen, W. and De Haes, S. Implementing Information Technology Governance: Models, Practices and Cases. IGI Publishing. Hershey, 2008.

Verhoef, C. Quantifying the effects of IT-governance rules. Science of Computer Programming, 2007.

W. R. Quint, ITIL V3. Amsterdã, 2008.

Weill, P.; Ross, J. A matrix approach to designing IT governance. Sloan Management Review, v. 46, n. 2, 2005.

Weill, P., Ross, J. W.: IT governance – How top performers manage IT decision rights for superior results. Harvard Business School Press, 2004.

White, Lilly T.P: implementing BS17799 in the UK national health service. Computer Fraud & Security. Issue, 2004.

Yin, Robert K.: Estudo de caso: planejamento e método - Porto Alegre, 2.ed:, 2001.

APÊNDICES

A – ANÁLISE DE DOCUMENTOS LEGAIS

INSTRUÇÃO NORMATIVA Nº 02, de 30 de abril de 2008. Dispõe sobre regras e diretrizes para a contratação de serviços, continuados ou não.
Seleção de determinações relacionadas a governança de TI
Art. 2º As contratações de que trata esta Instrução Normativa deverão ser precedidas de planejamento, em harmonia com o planejamento estratégico da instituição, que estabeleça os produtos ou resultados a serem obtidos, quantidades e prazos para entrega das parcelas, quando couber.
Art. 2º As contratações de que trata esta Instrução Normativa deverão ser precedidas de planejamento, em harmonia com o planejamento estratégico da instituição, que estabeleça os produtos ou resultados a serem obtidos, quantidades e prazos para entrega das parcelas, quando couber. Parágrafo único. O planejamento de que trata o caput, quando dispor sobre serviços de natureza intelectual, deverá observar ainda as seguintes diretrizes: I – (revogado). (Revogado pela Instrução Normativa nº 3, de 16 de outubro de 2009). II – definir papéis e responsabilidades dos atores e áreas envolvidas na contratação, tais como: a) ateste dos produtos e serviços; b) resolução de problemas; c) acompanhamento da execução dos trabalhos; d) gerenciamento de riscos; e) sugestão de aplicação de penalidades; f) avaliação da necessidade de aditivos contratuais; g) condução do processo de repactuação, quando for o caso.
Art. 14. A contratação de prestação de serviços será sempre precedida da apresentação do Projeto Básico ou Termo de Referência, que deverá ser preferencialmente elaborado por técnico com qualificação profissional pertinente às especificidades do serviço a ser contratado, devendo o Projeto ou o Termo ser justificado e aprovado pela autoridade competente.
Art. 15. O Projeto Básico ou Termo de Referência deverá conter: I - a justificativa da necessidade da contratação, dispondo, dentre outros, sobre:

INSTRUÇÃO NORMATIVA Nº 02, de 30 de abril de 2008. Dispõe sobre regras e diretrizes para a contratação de serviços, continuados ou não.
Seleção de determinações relacionadas a governança de TI
a) motivação da contratação; b) benefícios diretos e indiretos que resultarão da contratação; c) conexão entre a contratação e o planejamento existente; d) agrupamento de itens em lotes; e) critérios ambientais adotados, se houver; f) natureza do serviço, se continuado ou não; g) inexigibilidade ou dispensa de licitação, se for o caso; e h) referências a estudos preliminares, se houver. II - o objetivo, identificando o que se pretende alcançar com a contratação.
Art. 15º inciso VII - a metodologia de avaliação da qualidade e aceite dos serviços executados;
Art15º - XVII - o Acordo de Níveis de Serviços, sempre que possível, conforme modelo previsto no anexo II, deverá conter: a) os procedimentos de fiscalização e de gestão da qualidade do serviço, especificando-se os indicadores e instrumentos de medição que serão adotados pelo órgão ou entidade contratante; b) os registros, controles e informações que deverão ser prestados pela contratada; e c) as respectivas adequações de pagamento pelo não atendimento das metas estabelecidas.
Art. 31. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do contrato, devendo ser exercidos por um representante da Administração, especialmente designado na forma dos arts. 67 e 73 da Lei nº 8.666/93 e do art. 6º do Decreto nº 2.271/97.
Art. 34. A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos seguintes aspectos, quando for o caso: I – os resultados alcançados em relação ao contratado, com a verificação dos prazos de execução e da qualidade demandada; II - os recursos humanos empregados, em função da quantidade e da formação profissional exigida; III - a qualidade e quantidade dos recursos materiais utilizados; IV - a adequação dos serviços prestados à rotina de execução estabelecida;

INSTRUÇÃO NORMATIVA Nº 02, de 30 de abril de 2008. Dispõe sobre regras e diretrizes para a contratação de serviços, continuados ou não.
Seleção de determinações relacionadas a governança de TI
V - o cumprimento das demais obrigações decorrentes do contrato; e VI - a satisfação do público usuário.

NORMA COMPLEMENTAR – 02/IN01/DSIC/GSIPR **Objetivo: Definir a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.**
Seleção de determinações relacionadas a governança de TI
3.1.7 Selecionar as ações de segurança da informação e comunicações consideradas necessárias para o tratamento de riscos. (Alguns exemplos de ações de segurança da informação e comunicações são: Política de Segurança da Informação e Comunicações, infraestrutura de segurança da informação e comunicações, tratamento da informação, segurança em recursos humanos, segurança física, segurança lógica, controle de acesso, segurança de sistemas, tratamento de incidentes, gestão de continuidade, conformidade, auditoria interna, além de outras que serão exploradas em outras normas complementares).
3.2.1 Formular um plano de metas para cada objetivo das ações de segurança da informação e comunicações aprovadas na fase do planejamento em ordem de prioridade, incluindo a atribuição de responsabilidades, os prazos para execução, e os custos estimados.
3.2.3 Implementar o plano de metas para atender as ações de segurança da informação e comunicações aprovadas.
3.2.4 Definir como medir a eficácia das ações de segurança da informação e comunicações, estabelecendo indicadores mensuráveis para as metas aprovadas.
3.2.5 Implementar programas de conscientização e treinamento, sendo necessário: a) assegurar que todo pessoal que tem responsabilidades atribuídas no plano de metas receba o treinamento adequado para desempenhar suas tarefas; b) manter registros sobre habilidades, experiências e qualificações do efetivo do órgão ou entidade relativos à segurança da informação e comunicações; c) assegurar que todo efetivo do órgão ou entidade esteja consciente da relevância e importância da segurança da informação e comunicações em suas atividades e como cada pessoa pode contribuir para o alcance dos objetivos das ações de segurança da informação e comunicações;

NORMA COMPLEMENTAR – 02/IN01/DSIC/GSIPR **Objetivo: Definir a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.**
Seleção de determinações relacionadas a governança de TI
3.1.7 Selecionar as ações de segurança da informação e comunicações consideradas necessárias para o tratamento de riscos. (Alguns exemplos de ações de segurança da informação e comunicações são: Política de Segurança da Informação e Comunicações, infraestrutura de segurança da informação e comunicações, tratamento da informação, segurança em recursos humanos, segurança física, segurança lógica, controle de acesso, segurança de sistemas, tratamento de incidentes, gestão de continuidade, conformidade, auditoria interna, além de outras que serão exploradas em outras normas complementares).
3.2.6 Gerenciar a execução das ações de segurança da informação e comunicações.
3.2.7 Gerenciar os recursos empenhados para o desenvolvimento das ações de segurança da informação e comunicações.
3.2.7 Implementar procedimentos capazes de permitir a pronta detecção de incidentes de segurança da informação e comunicações, bem como a resposta a incidentes de segurança da informação e comunicações.
3.3.1 Executar procedimentos de avaliação e análise crítica, a fim de: a) detectar erros nos resultados de processamento; b) identificar incidentes de segurança da informação e comunicações; c) determinar se as ações de segurança da informação e comunicações delegadas a pessoas ou implementadas por meio de tecnologia da informação e comunicações estão sendo executadas conforme planejado; d) determinar a eficácia das ações de segurança da informação e comunicações adotadas, mediante o uso de indicadores;
3.3.2 Realizar análises críticas regulares, a intervalos planejados de pelo menos uma vez por ano;
3.3.4 Atualizar a avaliação/análise de riscos a intervalos planejados de pelo menos uma vez por ano;
3.3.5 Conduzir auditoria interna, também denominada auditoria de primeira parte, das ações de segurança da informação e comunicações a intervalos planejados de pelo menos uma vez ao ano;
3.3.6 Atualizar os planos de segurança da informação e comunicações, considerando os resultados da avaliação e análise de crítica;
3.4.1 Propor à autoridade decisória de seu órgão ou entidade a necessidade de implementar as melhorias identificadas.
3.4.2 Executar as ações corretivas ou preventivas de acordo com a identificação de não conformidade real ou potencial;
3.4.3 Comunicar as melhorias à autoridade decisória de seu órgão ou entidade; e
3.4.4 Assegurar-se de que as melhorias atinjam os objetivos pretendidos.

NORMA COMPLEMENTAR - 03/IN01/DSIC/GSIPR **Objetivo: Estabelecer diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.**
Seleção de determinações relacionadas a governança de TI
5.1 Recomenda-se que para a elaboração da POSIC seja instituído um Grupo de Trabalho constituído por representantes dos diferentes setores do órgão ou entidade da APF, como por exemplo: segurança patrimonial, tecnologia da informação, recursos humanos, jurídico, financeiro e planejamento;
5.2 A elaboração da POSIC deve levar em consideração a natureza e finalidade do órgão ou entidade da APF, alinhando-se sempre que
5.2 A elaboração da POSIC deve levar em consideração a natureza e finalidade do órgão ou entidade da APF, alinhando-se sempre que possível à sua missão e ao planejamento estratégico;
5.3 Recomenda-se que na elaboração da POSIC sejam incluídos os seguintes itens:
5.3.1 **Escopo**: neste item recomenda-se descrever o objetivo e abrangência da Política de Segurança da Informação e Comunicações, definindo o limite no qual as ações de segurança da informação e comunicações serão desenvolvidas no órgão ou entidade da APF;
5.3.2 Conceitos e definições: neste item recomenda-se relacionar todos os conceitos e suas definições a serem utilizados na Política de Segurança da Informação e Comunicações do órgão ou entidade da APF que possam gerar dificuldades de interpretações ou significados ambíguos;
5.3.3 Referências legais e normativas: neste item recomenda-se relacionar as referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicações do órgão ou entidade da APF;
5.3.4 Princípios: neste item recomenda-se relacionar os princípios que regem a segurança da informação e comunicações no órgão ou entidade da APF;
5.3.5 Diretrizes Gerais: neste item recomenda-se estabelecer diretrizes sobre, no mínimo, os seguintes temas, considerando as Normas específicas vigentes no ordenamento jurídico: a) Tratamento da Informação; b) Tratamento de Incidentes de Rede; c) Gestão de Risco; d) Gestão de Continuidade; e) Auditoria e Conformidade; f) Controles de Acesso; g) Uso de e-mail; e h) Acesso a Internet.
5.3.6 Penalidades: neste item identificam-se as consequências e penalidades para os casos de violação da Política de Segurança da Informação e Comunicações ou de quebra de segurança, devendo ser proposto um termo de responsabilidade;
5.3.7 Competências e Responsabilidades: neste item recomendam-se os seguintes procedimentos:

5.3.7.1 Definir a estrutura para a Gestão da Segurança da Informação e Comunicações;
5.3.7.2 Instituir o Gestor de Segurança da Informação e Comunicações do órgão ou entidade da APF, dentre servidores públicos civis ou militares, conforme o caso, com as seguintes responsabilidades: a) Promover cultura de segurança da informação e comunicações; b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança; c) Propor recursos necessários às ações de segurança da informação e comunicações; d) Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes computacionais; e) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações; f) Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações; g) Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF.
5.3.7.3 Instituir o Comitê de Segurança da Informação e Comunicações do órgão ou entidade da APF com as seguintes responsabilidades: a) Assessorar na implementação das ações de segurança da informação e comunicações no órgão ou entidade da APF; b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; e c) Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.
5.3.7.4 Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do órgão ou entidade da APF.
5.3.8 Atualização: neste item recomenda-se estabelecer a periodicidade da revisão da Política de Segurança da Informação e Comunicações ou dos instrumentos normativos gerados a partir da própria POSIC.
5.4 A POSIC precisa ser objetiva, simples, de fácil leitura e entendimento;
5.5 A POSIC poderá ser complementada por Normas e Procedimentos que a referenciem.
6.1 Implementar a POSIC através da formalização e da aprovação por parte da autoridade máxima responsável pelo órgão ou entidade da APF, demonstrando a todos os servidores e usuários o seu comprometimento;
6.2 Garantir a provisão dos recursos necessários para a implementação da POSIC por parte do órgão ou entidade da APF;
6.3 Promover no órgão ou entidade da APF, a cultura de segurança da informação e comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização.
A POSIC e suas atualizações deverão ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e terceirizados que habitualmente trabalham no órgão ou entidade da APF.
Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03(três) anos.

NORMA COMPLEMENTAR - 04/IN01/DSIC/GSIPR Objetivo: Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF.
Seleção de determinações relacionadas a governança de TI
4.1 As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão ou entidade da Administração Pública Federal, direta e indireta – APF, além de estarem alinhadas à respectiva Política de Segurança da Informação e Comunicações do órgão ou entidade;
4.2 O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações;
4.3 O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deve estar alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar nº 02/DSIC/GSIPR, publicada no Diário Oficial da União nº 199, Seção 1, de 14 de outubro de 2008, de modo a fomentar a sua melhoria contínua;
4.4 A Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC deverá produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios.
Uma abordagem sistemática do processo Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, com o objetivo de manter os riscos em níveis aceitáveis, deve conter:
5.1 Definições preliminares: nesta fase, deve-se realizar uma análise da organização visando estruturar o processo de gestão de riscos de segurança da informação e comunicações, sendo consideradas as características do órgão ou entidade e as restrições a que estão sujeitas. 5.1.1 Definir o escopo de aplicação da Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC a fim de delimitar o âmbito de atuação. Esse escopo pode abranger o órgão ou entidade como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação; 5.1.2 Adotar uma metodologia de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC que atenda aos objetivos, diretrizes gerais e o escopo definido contemplando, no mínimo, os critérios de avaliação e de aceitação do risco.
5.2 Análise/avaliação dos riscos: nesta fase, inicialmente serão identificados os riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados. 5.2.1 Identificar os ativos e seus respectivos responsáveis dentro do escopo estabelecido; 5.2.2 Identificar os riscos associados ao escopo definido, considerando: a) as ameaças envolvidas; b) as vulnerabilidades existentes nos ativos de informação; c) as ações de Segurança da Informação e Comunicações – SIC já adotadas. 5.2.3 Estimar os riscos levantados, considerando os valores ou níveis para a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados; 5.2.4 Avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento, comparando a estimativa de riscos com os critérios estabelecidos no item 5.1.2;

NORMA COMPLEMENTAR - 04/IN01/DSIC/GSIPR Objetivo: Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF.
Seleção de determinações relacionadas a governança de TI
5.2.5 Relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos pelo órgão ou entidade.
5.3 Plano de Tratamento dos Riscos 5.3.1 Determinar as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir ou reter o risco, observando: a) a eficácia das ações de Segurança da Informação e Comunicações – SIC já existentes; b) as restrições organizacionais, técnicas e estruturais; c) os requisitos legais; d) a análise custo/ benefício. 5.3.2 Formular um plano para o tratamento dos riscos, relacionando, no mínimo, as ações de Segurança da Informação e Comunicações – SIC, responsáveis, prioridades e prazos de execução necessários à sua implantação.
5.4 Aceitação do Risco: verificar os resultados do processo executado, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.
5.5 Implementação do Plano de Tratamento dos Riscos: executar as ações de Segurança da Informação e Comunicações – SIC incluídas no Plano de Tratamento dos Riscos aprovado.
5.6 Monitoração e análise crítica: detectar possíveis falhas nos resultados, monitorar os riscos, as ações de Segurança da Informação e Comunicações – SIC e verificar a eficácia do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC. 5.6.1 Do processo de gestão: monitorar e analisar criticamente o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC de forma a mantê-lo alinhado às diretrizes gerais estabelecidas e às necessidades do órgão ou entidade; 5.6.2 Do risco: manter os riscos monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças: a) nos critérios de avaliação e aceitação dos riscos; b) no ambiente; c) nos ativos de informação; d) nas ações de Segurança da Informação e Comunicações – SIC; e) nos fatores do risco (ameaça, vulnerabilidade, probabilidade e impacto).
5.7 Melhoria do Processo de GRSIC 5.7.1 Propor à autoridade decisória do órgão ou entidade a necessidade de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica; 5.7.2 Executar as ações corretivas ou preventivas aprovadas; 5.7.3 Assegurar que as melhorias atinjam os objetivos pretendidos.

NORMA COMPLEMENTAR - 04/IN01/DSIC/GSIPR
Objetivo: Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF.
Seleção de determinações relacionadas a governança de TI
5.8 Comunicação do Risco: manter as instâncias superiores informadas a respeito de todas as fases da gestão de risco, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas.

NORMA COMPLEMENTAR - 05/IN01/DSIC/GSIPR
Objetivo: Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Seleção de determinações relacionadas a governança de TI
Cada órgão ou entidade deverá estabelecer, dentre os modelos apresentados abaixo, aquele que melhor se adequar às suas necessidades e limitações, ressalvado que, independentemente do modelo escolhido, deverão ser observadas as diretrizes desta Norma Complementar.
7.1 Modelo 1 – Utilizando a equipe de tecnologia da informação – TI **7.1.1** Neste modelo não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes de Rede. A Equipe será formada a partir dos membros das equipes de TI do próprio órgão ou entidade, que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais. Neste modelo as funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos em segurança. **7.1.2** A Equipe que utilizar este modelo desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades pró-ativas.
7.2 Modelo 2 – Centralizado 7.2.1 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais será estabelecida de forma centralizada no âmbito da organização. 7.2.2 A Equipe será composta por pessoal com dedicação exclusiva às atividades de tratamento e resposta aos incidentes em redes computacionais.
7.3 Modelo 3 – Descentralizado 7.3.1 No modelo descentralizado a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais será composta por colaboradores distribuídos por diversos locais dentro da organização, dispersos por uma região ou pelo país inteiro. Essas equipes devem possuir pessoal próprio dedicado às atividades de tratamento e resposta aos incidentes de rede computacionais, podendo atuar operacionalmente de forma independente, porém alinhadas com as diretrizes estabelecidas pela coordenação

NORMA COMPLEMENTAR - 05/IN01/DSIC/GSIPR **Objetivo:** Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Seleção de determinações relacionadas a governança de TI
central. 7.3.2 A ETIR da organização será formada pelo conjunto dessas equipes distribuídas e chefiada pelo Agente Responsável designado.
7.4 Modelo 4 – Combinado ou Misto 7.4.1 Trata-se da junção dos modelos Descentralizado e Centralizado. Neste modelo existirá uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais central e Equipes distribuídas pela organização. 7.4.2 A Equipe central será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as Equipes descentralizadas, além de ser a responsável, perante toda a organização, pela comunicação com o CTIR GOV. 7.4.3 As Equipes distribuídas serão responsáveis por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade.
8.2 Os membros da Equipe deverão ser selecionados, sempre que possível, dentre o pessoal existente, com perfil técnico adequado às funções de tratamento de incidentes de rede, os quais deverão dedicar o tempo integral, ou um percentual do seu tempo de trabalho, dependendo do modelo de implementação adotado, de forma reativa e pró-ativa.
8.4 Recomenda-se que os membros da ETIR sejam: administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte ou quaisquer outras pessoas da organização com conhecimento técnico comprovado. A Equipe poderá ser estendida com a inclusão dos seguintes membros: representantes legais de áreas específicas da organização, advogados, estatísticos, recursos humanos, relações públicas, gestão de riscos, controle interno e grupo de investigação, ou outro que a organização entenda ser adequado.
8.5 Para cada membro da Equipe deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades da ETIR.
8.6 O Gestor de Segurança da Informação e Comunicações da organização será o responsável por prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe, bem como prover a infraestrutura necessária.
9 AUTONOMIA DA ETIR A autonomia da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR descreve o escopo de atuação e o nível de responsabilidade que a Equipe tem sobre as suas próprias ações e sobre as atividades de resposta e tratamento dos incidentes na rede de computadores. A autonomia define o nível de controle da Equipe no relacionamento com os componentes da sua organização. A autonomia deverá ser definida, explicitamente, no documento de constituição da ETIR, conforme apresentado no Anexo A desta Norma.
9.1 Autonomia Completa Se uma ETIR tem plena autonomia, ela poderá conduzir o seu público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança. Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

NORMA COMPLEMENTAR - 05/IN01/DSIC/GSIPR **Objetivo:** Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Seleção de determinações relacionadas a governança de TI
9.2 Autonomia Compartilhada 9.2.1 Se a ETIR possui a autonomia compartilhada, ela trabalhará em acordo com os outros setores da organização a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas. 9.2.2 A ETIR participará no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório. Neste caso, a Equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os outros membros da organização. 9.2.3 A indicação dos membros do processo decisório deverá ser definida explicitamente no documento de constituição da ETIR.
9.3 Sem Autonomia 9.3.1 Se uma Equipe não tem autonomia, só poderá agir com a autorização de um membro da organização com a autoridade para tal, designado no documento de constituição da ETIR. 9.3.2 A ETIR não terá autonomia para a tomada de decisões ou adoção de ações, podendo, no entanto, recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque, mas não terá um voto na decisão final. 9.3.3 A ETIR poderá ser capaz, devido à sua posição na organização e capacidade técnica, de conduzir os tomadores de decisão a agir durante um incidente de segurança, ressalvado o caráter sugestivo das recomendações.
10.1 Os órgãos ou entidades que inicialmente optarem pela implantação do Modelo 1 (Utilizando a equipe de tecnologia da informação) deverão, assim que possível, migrar para um dos outros modelos.
10.2 Preferencialmente a Equipe deve ser composta por servidores públicos ocupantes de cargo efetivo ou militares de carreira, conforme o caso, com perfil técnico compatível, lotados nos seus respectivos órgãos.
10.3 Cada órgão poderá deliberar o nome de sua Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.
10.4 A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV.
10.5 A ETIR poderá usar as melhores práticas de mercado, desde que não conflitem com os dispositivos desta Norma Complementar.
10.6 A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.
10.7 A troca de informações e a forma de comunicação entre as ETIR, e entre estas e o CTIR GOV, serão formalizadas caso a caso, se necessário, por Termo de Cooperação Técnica.

NORMA COMPLEMENTAR - 06/IN01/DSIC/GSIPR **Objetivo:** Estabelecer diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Seleção de determinações relacionadas a governança de TI
5.1 A elaboração do Programa de Gestão da Continuidade de Negócios envolve os seguintes procedimentos: 5.1.1 desenvolver documento com as diretrizes do Programa de Continuidade; 5.1.2 definir as atividades críticas do órgão ou entidade; 5.1.3 avaliar os riscos a que estas atividades críticas estão expostas; 5.1.4 definir as estratégias de continuidade para as atividades críticas; 5.1.5 desenvolver e implementar os Planos previstos no Programa de Gestão da Continuidade de Negócios para respostas tempestivas a interrupções; 5.1.6 realizar exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias; 5.1.7 desenvolver a cultura de continuidade de negócios no órgão ou entidade;
5.2 Os procedimentos previstos no Programa de Gestão da Continuidade de Negócios são executados em conformidade com os requisitos de segurança da informação e comunicações necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, o que inclui as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação e comunicações;
5.3 Recomenda-se que o Programa de Gestão de Continuidade de Negócios de um órgão ou entidade da APF seja composto, no mínimo, pelos seguintes Planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas: 5.3.1 Plano de Gerenciamento de Incidentes - PGI; 5.3.2 Plano de Continuidade de Negócios - PCN; 5.3.3 Plano de Recuperação de Negócios - PRN.
5.4 Cada um dos Planos contém, no mínimo:
5.4.1 Plano de Gerenciamento de Incidentes: a) Objetivo e escopo; b) papéis e responsabilidades; c) condições para a ativação de Planos; d) autoridade responsável; e) detalhes de contato; f) lista de tarefas e ações; g) atividades das pessoas;

NORMA COMPLEMENTAR - 06/IN01/DSIC/GSIPR **Objetivo:** Estabelecer diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Seleção de determinações relacionadas a governança de TI
5.1 A elaboração do Programa de Gestão da Continuidade de Negócios envolve os seguintes procedimentos: 5.1.1 desenvolver documento com as diretrizes do Programa de Continuidade; 5.1.2 definir as atividades críticas do órgão ou entidade; 5.1.3 avaliar os riscos a que estas atividades críticas estão expostas; 5.1.4 definir as estratégias de continuidade para as atividades críticas; 5.1.5 desenvolver e implementar os Planos previstos no Programa de Gestão da Continuidade de Negócios para respostas tempestivas a interrupções; 5.1.6 realizar exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias; 5.1.7 desenvolver a cultura de continuidade de negócios no órgão ou entidade;
5.2 Os procedimentos previstos no Programa de Gestão da Continuidade de Negócios são executados em conformidade com os requisitos de segurança da informação e comunicações necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, o que inclui as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação e comunicações;
h) Comunicação à mídia; i) Localização para o gerenciamento de incidentes.
5.4.2 Plano de Continuidade de Negócios: a) Objetivo e escopo; b) Papeis e responsabilidades; c) Autoridade responsável; d) Detalhes de contato; e) Lista de tarefas; f) Recursos necessários.
5.4.3 Plano de Recuperação de Negócios: a) Objetivo e escopo; b) Papéis e responsabilidades; c) Autoridade responsável; d) Detalhes de contato; e) Lista de tarefas;

NORMA COMPLEMENTAR - 06/IN01/DSIC/GSIPR **Objetivo:** Estabelecer diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Seleção de determinações relacionadas a governança de TI
5.1 A elaboração do Programa de Gestão da Continuidade de Negócios envolve os seguintes procedimentos: 5.1.1 desenvolver documento com as diretrizes do Programa de Continuidade; 5.1.2 definir as atividades críticas do órgão ou entidade; 5.1.3 avaliar os riscos a que estas atividades críticas estão expostas; 5.1.4 definir as estratégias de continuidade para as atividades críticas; 5.1.5 desenvolver e implementar os Planos previstos no Programa de Gestão da Continuidade de Negócios para respostas tempestivas a interrupções; 5.1.6 realizar exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias; 5.1.7 desenvolver a cultura de continuidade de negócios no órgão ou entidade;
5.2 Os procedimentos previstos no Programa de Gestão da Continuidade de Negócios são executados em conformidade com os requisitos de segurança da informação e comunicações necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, o que inclui as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação e comunicações;
f) Recursos necessários.
5.5 Os Planos são exercitados e testados periodicamente, bem assim os resultados documentados de forma a garantir a sua efetividade.
5.6 A revisão dos Planos é realizada nas seguintes situações: 5.6.1 No mínimo, uma vez por ano; 5.6.2 Em função dos resultados dos testes realizados; ou 5.6.3 Após alguma mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.
6.1 Para a Alta Administração do órgão ou entidade da APF, no âmbito de suas atribuições, recomenda-se que sejam adotadas as seguintes responsabilidades: 6.1.1 aprovar as diretrizes estratégicas que norteiam a elaboração do Programa de Gestão de Continuidade de Negócios; 6.1.2 avaliar a relação custo / benefício das estratégias de continuidade propostas e dos Planos que compõem o Programa de Gestão da Continuidade de Negócios e decida sobre sua implementação; 6.1.3 garantir os recursos necessários para estabelecer, implementar, operar e manter o Programa de Gestão da Continuidade de Negócios.
6.2 As seguintes atribuições devem ser conferidas ao responsável pela Gestão da Continuidade de Negócios, ou ao Gestor de Segurança da Informação e Comunicações, no caso do órgão ou entidade não possuir o Gestor de Continuidade de Negócios; 6.2.1 Propor as diretrizes estratégicas do Programa de Gestão da Continuidade de Negócios; 6.2.2 Avaliar o plano de tratamento de riscos;

NORMA COMPLEMENTAR - 06/IN01/DSIC/GSIPR **Objetivo:** Estabelecer diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Seleção de determinações relacionadas a governança de TI
5.1 A elaboração do Programa de Gestão da Continuidade de Negócios envolve os seguintes procedimentos: 5.1.1 desenvolver documento com as diretrizes do Programa de Continuidade; 5.1.2 definir as atividades críticas do órgão ou entidade; 5.1.3 avaliar os riscos a que estas atividades críticas estão expostas; 5.1.4 definir as estratégias de continuidade para as atividades críticas; 5.1.5 desenvolver e implementar os Planos previstos no Programa de Gestão da Continuidade de Negócios para respostas tempestivas a interrupções; 5.1.6 realizar exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias; 5.1.7 desenvolver a cultura de continuidade de negócios no órgão ou entidade;
5.2 Os procedimentos previstos no Programa de Gestão da Continuidade de Negócios são executados em conformidade com os requisitos de segurança da informação e comunicações necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, o que inclui as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação e comunicações;
6.2.3 Realizar, periodicamente, a Análise de Impacto nos Negócios (AIN); 6.2.4 Propor melhorias na implantação de novos controles relativos ao Programa de Gestão de Continuidade de Negócios; 6.2.5 Supervisionar a elaboração, implementação, testes e atualização dos Planos; 6.2.6 Desenvolver a cultura de Gestão de Continuidade de Negócios.
6.3 As seguintes atribuições devem ser conferidas aos responsáveis pelos setores ou processos onde foram identificadas atividades críticas para o órgão ou entidade da APF: 6.3.1 Elaborar os Planos previstos no Programa de Gestão da Continuidade de Negócios relacionados às atividades críticas; 6.3.2 Realizar os testes e exercícios dos Planos; 6.3.3 Avaliar e aprimorar os Planos a partir dos resultados dos testes e exercícios; 6.3.4 Administrar a contingência quando da interrupção de atividades, com base nos Planos desenvolvidos;
6.3.5 Propor os recursos necessários para a implantação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes e dos exercícios dos Planos.

NORMA COMPLEMENTAR - 07/IN01/DSIC/GSIPR **Objetivo:** Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da

Administração Pública Federal, direta e indireta - APF.
Seleção de determinações relacionadas a governança de TI
5.1 Quanto à criação e administração de contas de acesso:
5.1.1 A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para qualquer usuário.
5.1.2 Disponibilizar ao usuário, que não exerce funções de administração da rede local, somente uma única conta institucional de acesso, pessoal e intransferível.
NORMA COMPLEMENTAR - 07/IN01/DSIC/GSIPR **Objetivo:** Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.
5.1.3 Utilizar conta de acesso no perfil de administrador somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.
5.1.4 Responsabilizar o usuário pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso, mediante assinatura de Termo de Responsabilidade (Modelo - AnexoA). 5.1.5 A criação de contas de serviço exige regras específicas vinculadas a um processo automatizado.
5.1.6 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para credenciamento, bloqueio e exclusão de contas de acesso de seus usuários, bem como para o ambiente de desenvolvimento.
5.2 Quanto à rede corporativa de computadores:
5.2.1 Conceder credenciais de acesso à rede corporativa de computadores após a data de contratação ou de entrada em exercício do usuário.
5.2.2 Excluir credenciais de acesso à rede corporativa de computadores quando do desligamento do usuário.
5.2.3 Registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em cada órgão ou entidade da APF.
5.2.4 Implementar, sempre que possível, pelo menos um dos mecanismos que contemplam biometria, tokens, smart cards, a fim de autenticar a identidade do usuário da rede.
5.2.5 Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores.
5.2.6 Manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.
5.2.7 Utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.
5.2.8 Gravar o acesso remoto à rede corporativa em logs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada;
5.2.9 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso de redes sem fio.
5.3 Quanto aos ativos de informação:
5.3.1 Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.

5.3.2 Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;
5.3.3 Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia;
5.3.4 Registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas.
5.3.5 Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.
5.3.6 O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade públicas será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.
5.3.7 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso da Internet, do Correio Eletrônico e de Mensagens Instantâneas.
NORMA COMPLEMENTAR - 07/IN01/DSIC/GSIPR **Objetivo:** Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.
6. DIRETRIZES PARA CONTROLE DE ACESSO FÍSICO
6.1 Quanto às áreas e instalações físicas:
6.1.1 Os Órgãos ou entidades da APF estabelecem regras para o uso de credenciais físicas (crachá, botom, cartões, selos, etc,), que se destinam ao controle de acesso dos usuários às áreas e instalações sob suas responsabilidades;
6.1.2 Os Órgãos ou entidades da APF definem a necessidade e orientam a instalação de sistemas de detecção de intrusos nas áreas e instalações sob suas responsabilidades;
6.1.3 Classificar as áreas e instalações como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações, mapeando aquelas áreas e instalações consideradas críticas;
6.1.4 Os Órgãos ou entidades da APF orientam o uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída;
6.1.5 Proteger os ativos de informação contra ações de vandalismo, sabotagem, ataques, etc, especialmente em relação àqueles considerados críticos.
6.1.6 Implementar área de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais;
6.1.7 Definir pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado;
6.1.8 Intensificar os controles para as áreas e instalações consideradas críticas em conformidade com a legislação vigente.
6.2 Quanto aos usuários:
6.2.1 Difundir e exigir o cumprimento da Política de Segurança da Informação e Comunicações, das normas de segurança e da legislação vigente acerca do tema;
6.2.2 Conscientizar o usuário para adotar comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações.
6.2.3 Identificar e avaliar sistematicamente os riscos à segurança da informação e comunicações dos ativos de informação e quais controles devem ser aplicados quanto aos acessos dos usuários;
6.2.4 Estabelecer formulário específico de Termo de Responsabilidade (Modelo - Anexo A) a ser difundido e assinado individualmente pelos usuários;
6.2.5 Definir regras específicas para autorização de acesso e credenciamento dos usuários em conformidade com a classificação dos ativos de informação.

6.3 Quanto aos ativos de informação:
6.3.1 Estabelecer distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups);
6.3.2 Classificar os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios relativas aos aspectos da segurança da informação e comunicações da APF.
6.3.4 Os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com a legislação vigente.
NORMA COMPLEMENTAR - 07/IN01/DSIC/GSIPR **Objetivo:** Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.
6.4 Quanto ao perímetro de segurança:
6.4.1 Definir perímetros de segurança, suas dimensões, equipamentos e tipos especiais de controles de acesso aos ativos de informação;
6.4.2 Ilustrar em documentação própria e permitir que sejam identificados os perímetros de segurança de cada ativo de informação por todos que transitarem ou tiverem acesso em tais espaços, em especial às áreas e instalações consideradas críticas;
6.4.3 Regulamentar, por intermédio de normas específicas de cada órgão ou entidade da APF, o armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetros de segurança.

NORMA COMPLEMENTAR 08/IN01/DSIC/GSIPR, DE 19 DE AGOSTO DE 2010. Objetivo: Disciplinar o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.
Seleção de determinações relacionadas a governança de TI
7 GESTÃO DOS SERVIÇOS Para a definição dos serviços que serão prestados cada órgão deverá observar as suas necessidades e limitações, a missão, o modelo de implementação adotado e a autonomia da ETIR;
7.1 Recomenda-se que a ETIR defina os serviços a serem oferecidos à sua comunidade e, na medida em que forem oferecidos, que o sejam de forma gradativa e de acordo com a maturidade da equipe;
7.2 Além do serviço de tratamento de incidentes de segurança em redes de computadores, a ETIR poderá oferecer à sua comunidade um ou mais dos serviços listados a seguir, sem prejuízo de outros requisitados, desde que em consonância com normas e legislações referentes ao gerenciamento de incidentes de segurança em redes de computadores: 7.2.1 Tratamento de artefatos maliciosos;

NORMA COMPLEMENTAR 08/IN01/DSIC/GSIPR, DE 19 DE AGOSTO DE 2010. Objetivo: Disciplinar o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.
Seleção de determinações relacionadas a governança de TI
7.2.2 Tratamento de vulnerabilidades; 7.2.3 Emissão de alertas e advertências; 7.2.4 Anúncios; 7.2.5 Prospecção ou monitoração de novas tecnologias; 7.2.6 Avaliação de segurança; 7.2.7 Desenvolvimento de ferramentas de segurança; 7.2.8 Detecção de intrusão; 7.2.9 Disseminação de informações relacionadas à segurança;
7.3 Descrição, puramente exemplificativa, dos possíveis serviços de tratamento de incidentes de segurança em redes de computadores, não esgotando a possibilidade de implementação de outros serviços inerentes às peculiaridades da ETIR:
7.3.1 Tratamento de artefatos maliciosos - Este serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou em qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido o artefato o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa contra estes artefatos;
7.3.2 Tratamento de vulnerabilidades - Este serviço prevê o recebimento de informações sobre vulnerabilidades, quer sejam em *hardware* ou *software*, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção dessas vulnerabilidades;
7.3.3 Emissão de alertas e advertências - Este serviço consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores ocorrido, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema;
7.3.4 Anúncios - Este serviço consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral, cujos impactos sejam de médio e longo prazo, possibilitando que a comunidade se prepare contra novas ameaças;
7.3.5 Prospecção ou monitoração de novas tecnologias - Este serviço prospecta e/ou monitora o uso de novas técnicas das atividades de intrusão e tendências relacionadas, as quais ajudarão a identificar futuras ameaças. Este serviço inclui a participação em listas de discussão sobre incidentes de segurança em redes de computadores e o acompanhamento de notícias na mídia em geral sobre o tema;
7.3.6 Avaliação de segurança - Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores da organização com base em requisitos da própria organização ou em melhores práticas de mercado. O serviço pode incluir: revisão da infraestrutura, revisão de processos, varredura da rede e testes de penetração;
7.3.7 Desenvolvimento de ferramentas de segurança - Este serviço consiste no desenvolvimento de qualquer ferramenta nova específica de tratamento de incidentes de segurança em redes de computadores, para a ETIR ou para comunidade;

NORMA COMPLEMENTAR 08/IN01/DSIC/GSIPR, DE 19 DE AGOSTO DE 2010. Objetivo: Disciplinar o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.
Seleção de determinações relacionadas a governança de TI
7.3.8 Detecção de intrusão - Este serviço prevê a análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta a incidente de segurança em redes de computadores, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão e, ainda, possibilitar o envio de alerta em consonância com padrão de comunicação previamente definido entre a ETIR e o CTIR Gov.
Toda ETIR deve observar e adotar, no mínimo, os seguintes aspectos e procedimentos:
8.1 Registro de incidentes de segurança em redes de computadores: todos os incidentes notificados ou detectados devem ser registrados, com a finalidade de assegurar registro histórico das atividades da ETIR;
8.2 Tratamento da informação: o tratamento da informação pela ETIR deve ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;
8.3 Recursos disponíveis: a ETIR deve possuir os recursos materiais, tecnológicos e humanos, suficientes para prestar os serviços oferecidos para sua comunidade;
8.4 Capacitação dos membros da ETIR: os membros da ETIR devem estar capacitados para operar os recursos disponíveis para a condução dos serviços oferecidos para a sua comunidade;
8.5 Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, as ETIR têm como dever, sem prejuízo do disposto no item 6 desta Norma Complementar e do item 10.6 da Norma Complementar nº 05/IN01/DSIC/GSIPR: 8.5.1 Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários; 8.5.2 Observar os procedimentos para preservação das evidências exigindo consulta às orientações sobre cadeia de custódia, conforme ato normativo específico a ser expedido; 8.5.3 Priorizar a continuidade dos serviços da ETIR e da missão institucional da organização, observando os procedimentos previstos no item 8.5.2.
NORMA COMPLEMENTAR 09/IN01/DSIC/GSIPR, DE 19 DE NOVEMBRO DE 2010. Objetivo: Estabelecer orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta (APF).
Seleção de determinações relacionadas a governança de TI
5.5 A cifração e decifração de informações classificadas e sigilosas devem utilizar recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros mínimos estabelecidos no Anexo B.

NORMA COMPLEMENTAR 08/IN01/DSIC/GSIPR, DE 19 DE AGOSTO DE 2010. Objetivo: Disciplinar o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.
Seleção de determinações relacionadas a governança de TI
5.6 Todo recurso criptográfico constitui uma informação classificada sigilosa e requer procedimentos especiais de controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação pertinente;

NORMA COMPLEMENTAR 10/IN01/DSIC/GSIPR, DE 30 DE JANEIRO DE 2012. **Objetivo: Estabelecer diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.**
Seleção de determinações relacionadas a governança de TI
4.1 As diretrizes gerais do processo de Inventário e Mapeamento de Ativos de Informação devem considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais, e a estrutura do órgão ou entidade da APF, além do que devem estar alinhadas à Instrução Normativa GSIPR 01/2008, bem como à Política de Segurança da Informação e Comunicações do órgão ou entidade.
4.1.1 Tais diretrizes devem, também, subsidiar propostas de novos investimentos na área de segurança da Informação e Comunicações;
4.2 O processo de Inventário e Mapeamento de Ativos de Informação objetiva a Segurança das Infraestruturas Críticas de Informação do órgão ou entidade da APF, e deve ser aplicado tanto na Gestão de Riscos de Segurança da Informação e Comunicações, quanto na Estratégia de Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações;
4.3 O processo de Inventário e Mapeamento de Ativos de Informação deve subsidiar o órgão ou entidade da APF a conhecer, valorizar, proteger e manter seus ativos de informação, em conformidade com os requisitos legais e do negócio;
4.4 O processo de Inventário e Mapeamento de Ativos de Informação tem como objetivo prover o órgão ou entidade da APF: de um entendimento comum, consistente e inequívoco de seus ativos de informação; da identificação clara de seu(s) responsável(eis) - proprietário(s) e custodiante (s); de um conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo de informação; de uma descrição do contêiner de cada ativo de informação; e da identificação do valor que o ativo de informação representa para o negócio do órgão ou entidade da APF;
4.5 O processo de Inventário e Mapeamento de Ativos de Informação deve produzir subsídios tanto para a Gestão de Segurança da Informação e Comunicações, a Gestão de Riscos de Segurança da Informação e Comunicações, e a Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, da APF, quanto para os procedimentos de avaliação da conformidade, de melhorias contínuas, auditoria e, principalmente, de estruturação e geração de base de dados sobre os ativos de informação;
4.6 O processo de Inventário e Mapeamento de Ativos de Informação, deve ser dinâmico, periódico, e estruturado, para manter a Base de Dados de Ativos de

NORMA COMPLEMENTAR 10/IN01/DSIC/GSIPR, DE 30 DE JANEIRO DE 2012. **Objetivo: Estabelecer diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.**
Seleção de determinações relacionadas a governança de TI
Informação atualizada e consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações. Tal Base de Dados deve operar como infraestrutura material e técnica em condições de dar suporte às ações de cooperação entre entes federativos que têm sob as suas governança ativos de informação.
5 PROCEDIMENTOS O subprocesso de Identificação e Classificação de Ativos de Informação caracteriza-se por 6 (seis) etapas: (1) coleta de informações gerais dos ativos de informação; (2) detalhamento dos ativos de informação; (3) identificação do(s) responsável(is) – proprietário(s) e custodiante(s) de cada ativo de informação; (4) caracterização dos contêineres dos ativos de informação; (5) definição dos requisitos de segurança da informação e comunicações; e (6) estabelecimento do valor do ativo de informação.
5.1 Coleta de informações gerais dos ativos de informação
5.1.1 Recomenda-se definir o escopo da coleta, levantando no mínimo um conjunto essencial de informações sobre cada ativo de informação. Esse escopo pode abranger o órgão ou entidade da APF como um todo, um segmento, ou mesmo, um processo; e
5.1.2 Recomenda-se adotar metodologias de Gestão de Riscos de Segurança da Informação e Comunicações e de Gestão de Continuidade de Negócios, nos aspectos relacionados à SIC, que incorporem o processo de Inventário e Mapeamento de Ativos de Informação.
5.2 Detalhamento dos ativos de informação Recomenda-se, portanto, que o detalhamento inicial dos ativos de informação, contemple no mínimo um conjunto essencial de informações, e deva ser suficiente para:
5.2.1 determinar com clareza e objetividade o conteúdo do ativo de informação;
5.2.2 identificar o(s) responsável(is) – proprietário(s) e custodiante(s) - de cada ativo de informação;
5.2.3 identificar o valor de cada ativo de informação; e,
5.2.4 identificar os respectivos requisitos de segurança da informação e comunicações dos ativos de informação. Recomenda-se, que o detalhamento dos ativos de informação contemple também, e sempre que possível, o levantamento das interfaces e das interdependências internas e externas dos ativos de informação considerados críticos, dos órgãos ou entidades da APF, bem como os impactos quando da indisponibilidade ou destruição de tais ativos de informação, seja no caso de incidentes ou de desastres, visando atender os interesses da sociedade e do Estado.
5.3 Identificação do(s) responsável(is) – proprietário(s) e custodiante(s) - de cada ativo de informação
5.3.1 O proprietário do ativo de informação refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual

NORMA COMPLEMENTAR 10/IN01/DSIC/GSIPR, DE 30 DE JANEIRO DE 2012. **Objetivo: Estabelecer diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.**
Seleção de determinações relacionadas a governança de TI
é responsável primário pela viabilidade e sobrevivência dos ativos de informação;
5.3.2 O proprietário do ativo de informação deve assumir, no mínimo, as seguintes atividades: 1) descrever o ativo de informação; 2) definir as exigências de segurança da informação e comunicações do ativo de informação; 3) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários; 4) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo; e 5) indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação.
5.3.3 O custodiante do ativo de informação deve proteger um ou mais ativos de informação do órgão ou entidade da APF, como é armazenado, transportado e processado, de forma a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação. Ou seja, deve proteger os contêineres dos ativos de informação, e, consequentemente, aplicar os níveis de controles de segurança conforme as exigências de segurança da informação e comunicações, comunicadas pelo(s) proprietário(s) do(s) ativo(s) de informação.
5.4 Caracterização dos contêineres dos ativos de informação
5.4.1 O contêiner é o local onde "vive" o ativo de informação, e assim, recomenda-se que o mesmo seja caracterizado, no mínimo, com as seguintes informações: lista de todos os recipientes em que um ativo da informação é armazenado, transportado ou processado, e respectiva indicação dos responsáveis por manter estes recipientes;
5.5 Definição dos requisitos de segurança da informação e comunicações dos ativos de informação
5.5.1 Os requisitos de segurança da informação e comunicações dos ativos de informação devem ser definidos por meio de critérios que atendam a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.
5.5.2 Recomenda-se que os requisitos de segurança da informação e comunicações dos ativos de informação sejam categorizados, no mínimo, em 5 categorias de controle: a) tratamento da informação; b) controles de acesso físico e lógico; c) gestão de risco de segurança da informação e comunicações; d) tratamento e respostas a incidentes em redes computacionais, e, f) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação e comunicações.
5.6 Estabelecimento do valor do ativo de informação
5.6.1 Cabe ao(s) proprietário(s) dos ativos de informação indicar o valor do ativo para o negócio do órgão ou entidade da APF, considerando fatores do(s) risco(s) os quais os ativos possam estar expostos, como ameaça, vulnerabilidade e impacto;
5.6.2 O proprietário do ativo da informação deve indicar o valor do ativo, o qual deve refletir o quão cada ativo de informação é importante para a que organização alcance seus objetivos estratégicos, e o quão o ativo de informação é imprescindível aos interesses da sociedade e do Estado.

NORMA COMPLEMENTAR 10/IN01/DSIC/GSIPR, DE 30 DE JANEIRO DE 2012. **Objetivo: Estabelecer diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.**
Seleção de determinações relacionadas a governança de TI
6.1 Cabe à Alta Administração do órgão ou entidade da APF aprovar as diretrizes gerais e o processo de Inventário e Monitoramento de Ativos de Informação observada, dentre outros, a Política de Segurança da Informação e Comunicações e a Gestão de Riscos de Segurança da Informação e Comunicações, do órgão ou entidade da APF, bem como a sua missão e os seus objetivos estratégicos;
6.2 O Gestor de Segurança da Informação e Comunicações, no âmbito de suas atribuições, é responsável pela coordenação do Inventário e Mapeamento de Ativos de Informação nos órgãos ou entidades da APF, bem como pela indicação de Agente Responsável pela gerência de tais atividades. É responsável, também, pela análise quanto aos resultados obtidos de controle dos níveis de segurança da informação e comunicações de cada ativo de informação, e consequente, proposição de ajustes e de medidas preventivas e proativas à Alta Direção;
6.3 Cabe ao Agente Responsável, no mínimo, as seguintes atividades: o processo de identificação e classificação de ativos de informação; o monitoramento dos níveis de segurança dos ativos de informação junto aos proprietários e custodiantes dos ativos de informação; e, a elaboração sistemática de relatórios para os Gestores de Segurança da Informação e Comunicações.

NORMA COMPLEMENTAR 11/IN01/DSIC/GSIPR, DE 30 DE JANEIRO DE 2012. Estabelecer diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.
Seleção de determinações relacionadas a governança de TI
4 PRINCÍPIOS E DIRETRIZES
4.1 As diretrizes gerais para a avaliação de conformidade em segurança da informação e comunicações deverão considerar, no mínimo, as legislações vigentes a respeito de SIC para a APF e normativos internos específicos de cada órgão;
4.2 A avaliação de conformidade em SIC deve ser contínua e aplicada visando contribuir com a Gestão de Segurança da Informação e Comunicações dos órgãos e entidades da APF;
4.4 As não conformidades relativas ao descumprimento de legislações, normas e procedimentos são consideradas riscos de SIC e devem ser tratadas segundo a NC 04/IN01/GSIPR/DSIC;
4.5 Os responsáveis pela verificação de conformidade devem considerar os requisitos mínimos que assegurem a disponibilidade, integridade, confidencialidade e autenticidade das informações, observando, dentre outros, as legislações vigentes a respeito de SIC para a APF e normativos internos específicos de cada órgão;
4.6 Os responsáveis pela avaliação de conformidade devem ser capacitadas nas legislações vigentes referentes à segurança da informação e comunicações; e

4.7 A avaliação de conformidade de SIC tomará, no mínimo, como base no inventário e mapeamento de ativos de informação dos órgãos e entidades da APF, visando manter a disponibilidade, integridade, confidencialidade e autenticidade das informações.
5.1 Cabe à Alta Administração do órgão ou entidade da Administração Pública Federal, direta e indireta – APF aprovar as diretrizes para avaliação de conformidade em SIC;
5.2 Cabe ao Gestor de Segurança da Informação e Comunicações:
5.2.1 acompanhar se os procedimentos de SIC estão sendo aplicados de forma atender a conformidade com legislações vigentes a respeito de SIC para a APF e normativos internos específicos de cada órgão;
5.2.2 Promover ações de capacitação para os responsáveis pela avaliação de conformidade, visando que esses tenham conhecimento das legislações vigentes que tratam sobre o assunto de SIC.
5.3 Cabe ao responsável pela avaliação de conformidade remeter os resultados da avaliação de conformidade em SIC ao Gestor de Segurança da Informação e Comunicações.

NORMA COMPLEMENTAR 13/IN01/DSIC/GSIPR, DE 30 DE JANEIRO DE 2012. Estabelecer diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).
Seleção de determinações relacionadas a governança de TI
5 RESPONSABILIDADES E COMPETÊNCIAS
5.1 O Gestor de Segurança da Informação e Comunicações (Gestor de SIC) é o responsável pelas recomendações referentes às mudanças nos aspectos relativos à segurança da informação e comunicações, assim como, em observar todas as demais recomendações constantes nesta Norma Complementar. No processo de gerenciamento de mudanças, cabem-lhe as seguintes competências:
5.1.1 Avaliar os potenciais impactos à segurança da informação e comunicações que possam ocorrer durante a implementação da mudança;
5.1.2 Recomendar a implementação ou não das mudanças propostas, indicando, sempre que possível, soluções que mitiguem riscos à SIC;
5.1.3 Verificar se o andamento e o resultado da mudança viabilizam e asseguram a disponibilidade, integridade, confidencialidade e autenticidade da informação; e
5.1.4 Capacitar em SIC as equipes envolvidas com os processos de mudanças.
5.2 O Gestor de Mudanças, no âmbito de suas atribuições, é o responsável pelo planejamento e implementação das mudanças no âmbito do órgão ou entidade da APF, assim como, em observar todas as recomendações constantes nesta Norma Complementar.

5.3 Compete ao Gestor de Mudanças, no que tange à SIC, envolver o Gestor de SIC no processo de mudanças nos aspectos relativos à segurança da informação e comunicações, bem como envolver a gestão de risco de SIC e a gestão de continuidade de negócios em SIC do órgão ou entidade da APF.
6 PROCEDIMENTOS
6.1 Recomenda-se adotar uma metodologia de processo de gestão de mudanças que atenda, no mínimo, ao objetivo e às diretrizes gerais definidos nesta Norma Complementar.
6.2 Recomenda-se que o processo de gestão de mudanças seja composto, no mínimo, pelas fases de Descrição, Avaliação, Aprovação, Implementação e Verificação, de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, conforme detalhado a seguir:
6.2.1 Descrição: nesta fase, deve-se realizar uma descrição detalhada da mudança, contendo escopo, objetivo e benefícios de modo que, a partir dessa descrição, possa ser feita uma análise dos impactos à segurança da informação e comunicações. O escopo de aplicação da mudança pode abranger o órgão ou entidade como um todo, um segmento ou um ativo de informação.
6.2.2 **Avaliação**: nesta fase, são avaliados os potenciais impactos à segurança da informação e comunicações que possam ocorrer durante a implementação da mudança. Nesta fase deverão ser avaliados: a) Os detalhes do procedimento de implementação da mudança; b) A análise de risco do (s) ativo (s) de informação que serão afetados com a mudança; c) As legislações e normas pertinentes; d) A relação desta mudança com outras mudanças que possam estar ocorrendo simultaneamente; e) O impacto de adiar ou de não se fazer a mudança.
6.2.3 **Aprovação**: nesta fase, formaliza-se a aprovação ou não das mudanças propostas com base nas avaliações descritas no item 6.2.2.
6.2.4 **Implementação**: nesta fase, as mudanças aprovadas são agendadas e implementadas de acordo com o procedimento aprovado no item 6.2.3.
6.2.5 **Verificação**: esta fase transcorre paralelamente à fase de Implementação, e nela é verificado se o andamento e o resultado da mudança viabilizam e asseguram a disponibilidade, integridade, confidencialidade e autenticidade da informação.
6.3 Orienta-se ao Gestor de Mudanças observar, ainda, se o processo de gestão de mudanças contempla os seguintes procedimentos: a) Identificação e registro de todas as etapas das mudanças; b) Correta alocação dos recursos disponíveis; c) Planejamento e testes das mudanças; d) Comunicação dos detalhes das mudanças para todas as pessoas envolvidas; e e) Procedimentos de recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.
NORMA COMPLEMENTAR - 14/IN01/DSIC/GSIPR, DE 30 DE JANEIRO DE 2012. **Objetivo: Estabelecer diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e**

Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
Seleção de determinações relacionadas a governança de TI
5 PRINCÍPIOS E DIRETRIZES
5.1. O órgão ou entidade da APF deve observar, no mínimo, antes de adotar a tecnologia de computação em nuvem: 5.1.1. As diretrizes estabelecidas em sua POSIC; 5.1.2. As diretrizes do processo de Gestão de Riscos de SIC a respeito da adoção dos modelos de serviço e implementação de computação em nuvem; 5.1.3. As diretrizes do processo de Gestão de Continuidade de Negócios nos aspectos relacionados à SIC;
5.2. Ao contratar ou implementar um serviço de computação em nuvem, o órgão ou entidade da APF deve garantir que: 5.2.1. O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação estejam aderentes às diretrizes e normas de SIC, estabelecidas pelo GSIPR, e às legislações vigentes; 5.2.2. A legislação brasileira prevaleça sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações hospedadas na nuvem; 5.2.3. O contrato de prestação de serviço, quando for o caso, deve conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;
5.3. Os órgãos ou entidades da APF devem avaliar quais informações serão hospedadas na nuvem,considerando: 5.3.1. O processo de Classificação da Informação de acordo com a legislação vigente; 5.3.2. O valor do ativo de informação; 5.3.3. Os Controles de Acesso, físicos e lógicos, relativos à SIC; 5.3.4. O modelo de serviço e de implementação de computação em nuvem a serem adotados; 5.3.5. A localização geográfica onde as informações estarão fisicamente armazenadas.
6 RESPONSABILIDADES
6.1. Cabe à Alta Administração dos órgãos ou entidades da APF, no âmbito de suas competências, assegurar a utilização de tecnologias de computação em nuvem em conformidade com as orientações contidas nesta norma;
6.2. Ao Gestor de SIC, no âmbito de suas atribuições, cabe propor ações de SIC para a implementação ou a contração, nos órgãos ou entidades da APF, de tecnologias de computação em nuvem em conformidade com as orientações contidas nesta Norma Complementar;
6.3. De acordo com as necessidades de cada órgão ou entidade da APF, podem ser indicados agentes responsáveis pela implementação dos procedimentos relativos ao uso seguro de tecnologias de computação em nuvem em conformidade com as orientações contidas nesta Norma Complementar.
NORMA COMPLEMENTAR 15/IN01/DSIC/GSIPR, DE 11 DE JUNHO DE 2012 **Estabelecer diretrizes de Segurança da Informação e Comunicações para o uso das redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.**

Seleção de determinações relacionadas a governança de TI
5 PRINCÍPIOS E DIRETRIZES
5.2 A normatização interna de uso seguro das redes sociais deve estar alinhada tanto à Política de Segurança da Informação e Comunicações (POSIC) quanto aos objetivos estratégicos do órgão ou entidade. Também deve estabelecer diretrizes, critérios, limitações e responsabilidades na gestão do uso seguro das redes sociais, por usuários que tenham permissão para administrar perfis institucionais ou que possuam credencial de acesso para qualquer rede social, a partir da infraestrutura das redes de computadores da APF.
5.3 A Norma Interna do órgão ou entidade da APF também deve considerar os requisitos legais de segurança da informação e comunicações em vigor, especialmente as Normas Complementares NC 04/IN01/DSIC/GSIPR, que trata sobre a Gestão de Riscos de Segurança da Informação e Comunicações; NC 06/IN01/DSIC/GSIPR, sobre a Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações; NC 07/IN01/DSIC/GSIPR sobre Controles de Acesso Relativos à SIC e NC 08/IN01/DSIC/GSIPR, que estabelece Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da APF no que couber, bem como novas Normas Complementares do GSI referentes à SIC para a Administração Pública Federal.
5.5 É vedada a terceirização completa da administração e da gestão de perfis de órgãos e entidades da APF nas redes sociais, assim entendida a terceirização que viole o disposto no item anterior (5.4).
5.6 O órgão ou entidade da APF deve nomear um servidor público, ocupante de cargo efetivo ou militar de carreira, para a função de Agente Responsável pela gestão do uso seguro de cada perfil institucional nas redes sociais, com o seguinte perfil profissional: capacidade de estabelecer bons relacionamentos interpessoais, de interagir e dialogar com as demais áreas presentes nas redes sociais, proativo e, principalmente, que conheça e entenda o negócio do órgão ou entidade da APF a que esteja vinculado.
6 RESPONSABILIDADES
6.1 Cabe à Alta Administração aprovar as diretrizes estratégicas alinhadas à SIC, que norteiam o uso seguro das redes sociais do órgão ou entidade da APF de sua responsabilidade;
6.2 Cabe ao Comitê de Segurança da Informação e Comunicações, de cada órgão ou entidade analisar a Norma Interna de Uso Seguro das Redes Sociais e submeter à aprovação da Alta Administração.
6.3 Cabe ao Gestor de Segurança da Informação e Comunicações:
6.3.1 Propor diretrizes estratégicas de Segurança da Informação e Comunicações (SIC) para a gestão do uso seguro das redes sociais.
6.3.2 Fomentar o fortalecimento da cultura de Segurança da Informação e Comunicações do órgão ou entidade da Administração Pública Federal de sua responsabilidade, no que diz respeito ao uso seguro das redes sociais;
6.4 Cabe ao Agente Responsável:
6.4.1 Gerir, acompanhar e analisar, de forma contínua, o uso seguro das redes sociais pelo órgão ou entidade da APF;
6.4.2 Verificar se a Norma Interna de Uso Seguro das Redes Sociais está sendo seguida pelo órgão ou entidade;
6.4.3 Atuar como parceiro institucional no fortalecimento da cultura de SIC no uso seguro das redes sociais em seu órgão ou entidade, bem como no planejamento e

apoio às ações de segurança da informação e comunicações cabíveis nesse contexto.

Lei nº 6.404, DE 15 DE DEZEMBRO DE 1976.

LEI No 6.404, DE 15 DE DEZEMBRO DE 1976.

Art. 142. Compete ao conselho de administração:

I - fixar a orientação geral dos negócios da companhia;

II - eleger e destituir os diretores da companhia e fixar-lhes as atribuições, observado o que a respeito dispuser o estatuto;

III - fiscalizar a gestão dos diretores, examinar, a qualquer tempo, os livros e papéis da companhia, solicitar informações sobre contratos celebrados ou em via de celebração, e quaisquer outros atos;

IV - convocar a assembléia-geral quando julgar conveniente, ou no caso do artigo 132;

V - manifestar-se sobre o relatório da administração e as contas da diretoria;

VI - manifestar-se previamente sobre atos ou contratos, quando o estatuto assim o exigir;

VII - deliberar, quando autorizado pelo estatuto, sobre a emissão de ações ou de bônus de subscrição;

Lei 13.303, de 30 de junho de 2016 que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.

Art. 23. É condição para investidura em cargo de diretoria da empresa pública e da sociedade de economia mista a assunção de compromisso com metas e resultados específicos a serem alcançados, que deverá ser aprovado pelo Conselho de Administração, a quem incumbe fiscalizar seu cumprimento.

§ 1o Sem prejuízo do disposto no caput, a diretoria deverá apresentar, até a última reunião ordinária do Conselho de Administração do ano anterior, a quem compete sua aprovação:

I - plano de negócios para o exercício anual seguinte;

II - estratégia de longo prazo atualizada com análise de riscos e oportunidades para, no mínimo, os próximos 5 (cinco) anos.

Decreto 8.945, de 27 de dezembro de 2016, que regulamenta, no âmbito da União, a Lei no 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.

Art. 24. O estatuto social da empresa estatal deverá conter as seguintes regras mínimas:

I - constituição do Conselho de Administração, com, no mínimo, sete e, no máximo, onze membros;

II - definição de, no mínimo, um requisito específico adicional para o cargo de Diretor, em relação ao cargo de Conselheiro de Administração, observado o quantitativo mínimo de três Diretores;

III - avaliação de desempenho, individual e coletiva, de periodicidade anual, dos membros estatutários, observados os seguintes quesitos mínimos para os administradores:
a) exposição dos atos de gestão praticados quanto à licitude e à eficácia da ação administrativa;
b) contribuição para o resultado do exercício; e
c) consecução dos objetivos estabelecidos no plano de negócios e atendimento à estratégia de longo prazo;

IV - constituição obrigatória do Conselho Fiscal e funcionamento de modo permanente;
V - constituição obrigatória do Comitê de Auditoria Estatutário e funcionamento de modo permanente, ficando autorizada a criação de comitê único pelas empresas que possuam subsidiária em sua estrutura;
VI - prazo de gestão unificado para os membros do Conselho de Administração, não superior a dois anos, sendo permitidas, no máximo, três reconduções consecutivas;
VII - prazo de gestão unificado para os membros da Diretoria, não superior a dois anos, permitidas, no máximo, três reconduções consecutivas;
VIII - segregação das funções de Presidente do Conselho de Administração e Presidente da empresa; e
IX - prazo de atuação dos membros do Conselho Fiscal não superior a dois anos, sendo permitidas, no máximo, duas reconduções consecutivas.

Resolução CGPAR Nº-16, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR.

Art. 12 Além das atribuições definidas na legislação societária e no estatuto social,

compete ao Conselho de Administração das empresas estatais federais:
I - aprovar políticas gerais da empresa, inclusive de governança corporativa;
II - aprovar e acompanhar o plano estratégico, de investimentos e as metas de desempenho, que deverão ser apresentados pela diretoria;
III - analisar, ao menos trimestralmente, o balancete e demais demonstrações financeiras elaboradas periodicamente pela companhia, sem prejuízo da atuação do Conselho Fiscal;
IV - manifestar-se sobre as propostas a serem submetidas à deliberação dos acionistas em assembleia;
V - supervisionar os sistemas de gerenciamento de riscos e de controles internos;
VI - definir os assuntos e valores para alçada decisória do Conselho de Administração e da Diretoria;
VII - identificar a existência de ativos não de uso próprio da empresa e avaliar a necessidade de mantê-los;
VIII — aprovar a inclusão de matérias no instrumento de convocação da Assembleia Geral, não se admitindo a rubrica "assuntos gerais"; e
IX — deliberar sobre os casos omissos do estatuto social da empresa.
Parágrafo único. Ao longo de seu prazo de gestão, o Conselho de Administração deverá planejar as reuniões de modo a exercer todas as suas competências estatutárias.

Resolução CGPAR Nº-11, do Ministério do Planejamento, Orçamento e Gestão, Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União – CGPAR.

Art. 22As práticas de governança de TI devem incluir:
I — elaboração e acompanhamento de Plano Estratégico de Tecnologia da Informação
(PETI), aderente ao Plano Estratégico Institucional (PEI), dando-lhe ampla divulgação, à exceção de
informações classificadas como não públicas, nos termos da lei;
II — elaboração e acompanhamento de Plano Diretor de Tecnologia da Informação (PDTI), aderente ao PETI, dando-lhe ampla divulgação, à exceção de informações classificadas como não públicas, nos termos da lei;
III — definição e acompanhamento de indicadores e metas ligadas ao planejamento de TI,
baseados em parâmetros de governança e nas necessidades do negócio;
IV — estabelecimento de colegiado de nível estratégico de TI, formado por representantes
da alta administração, incluindo ao menos um Diretor estatutário, responsável por assegurar a adoção de
práticas estabelecidas nesta Resolução, pelo direcionamento estratégico de TI, e pela avaliação de seus principais investimentos;
V — estabelecimento de colegiado de nível tático, responsável, ao menos, pela definiçãodos investimentos seguindo as prioridades estabelecidas pelo colegiado de nível estratégico, pelo monitoramento de projetos e solução de conflitos, e pelo monitoramento dos níveis de serviço de TI e desua melhoria;
Art. 32 Devem ser estabelecidos procedimentos de controles internos, abrangendo os diversos níveis da organização, visando mitigar os riscos ligados, ao menos, aos seguintes processos:
I — Planejamento Estratégico Institucional (PEI);
III — Plano Diretor de TI (PDTI);
IV — funcionamento de comitês e fóruns ligados a TI;

V — processo orçamentário de TI;
VI — processo de software;
VII — gerenciamento de projetos de TI;
VIII — gerenciamento de serviços de TI;
IX — segurança da informação;
X — gestão de pessoal de TI;
XI — contrafação e gestão de soluções de TI;
XII — monitoramento do desempenho da TI organizacional.
Parágrafo único. Os controles internos devem ser periodicamente revisados e atualizados, de forma a serem incorporadas medidas relacionadas a riscos novos ou anteriormente não abordados.

INSTRUÇÃO NORMATIVA N° 4, DE 11 DE SETEMBRO DE 2014.

Art. 1º As contratações de Soluções de Tecnologia da Informação pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) serão disciplinadas por esta Instrução Normativa (IN).

§ 1º Esta IN não se aplica: I - às contratações cuja estimativa de preços seja inferior ao disposto no art. 23, inciso II, alínea "a" da Lei nº 8.666, de 21 de junho de 1993; II - às contratações dos Serviços Estratégicos de Tecnologia da Informação, que deverão observar o Plano de Capacidade, conforme disposto no inciso XIV do art. 2º desta IN, para confecção do Planejamento da Contratação nos termos da Lei, não se aplicando a estes casos os demais dispositivos desta IN, a exceção do disposto no § 2º deste artigo e do disposto no art. 4º desta IN, em que a contratada seja:
a) órgão ou entidade, nos termos do art. 24, inciso XVI da Lei nº 8.666, de 1993;
b) Empresa Pública, nos termos do art. 2º da Lei nº 5.615, de 13 de outubro de 1970, modificada pela Lei nº 12.249, de 11 de junho de 2010; e
c) Empresa Pública, nos termos da Lei nº 6.125, de 4 de novembro de 1974. III - às contratações de Soluções de Tecnologia da Informação que possam comprometer a segurança nacional, em que deverá ser observado o disposto no Decreto nº 8.135, de 4 de novembro de 2013, e suas regulamentações específicas.

Art. 4º As contratações de que trata esta IN deverão ser precedidas de planejamento,
elaborado em harmonia com o Plano Diretor de Tecnologia da Informação - PDTI.

§ 1º O PDTI deverá estar alinhado à EGTIC e ao plano estratégico institucional e
aprovado pelo Comitê de Tecnologia da Informação do órgão ou entidade.

§ 2º Inexistindo o PDTI, o órgão ou entidade deverá proceder à sua elaboração, observando, no que couber, o Guia de Elaboração de PDTI do SISP, acessível no Portal

do SISP. § 3º Inexistindo o plano estratégico institucional, sua ausência deverá ser registrada no PDTI e deverá ser utilizado um documento equivalente, como o Plano Plurianual - PPA. § 4º O Comitê de Tecnologia da Informação declarará quais são os Serviços Estratégicos de Tecnologia da Informação e quais são as Soluções de Tecnologia da Informação que possam comprometer a segurança nacional para fins de atendimento ao disposto no § 1º do art. 1º desta IN.

Art. 5º Não poderão ser objeto de contratação: I - mais de uma Solução de Tecnologia da Informação em um único contrato; e II - gestão de processos de Tecnologia da Informação, incluindo gestão de segurança da informação. Parágrafo único. O apoio técnico aos processos de planejamento e avaliação da qualidade das Soluções de Tecnologia da Informação poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do órgão ou entidade. Art. 6º Nos casos em que a avaliação, mensuração ou apoio à fiscalização da Solução de Tecnologia da Informação seja objeto de contratação, a contratada que provê a Solução de Tecnologia da Informação não poderá ser a mesma que a avalia, mensura ou apoia à fiscalização.

Art. 7º É vedado: I - estabelecer vínculo de subordinação com funcionários da contratada; II - prever em edital a remuneração dos funcionários da contratada; III - indicar pessoas para compor o quadro funcional da contratada; IV - demandar a execução de serviços ou tarefas que escapem ao escopo do objeto da contratação, mesmo que haja assentimento do preposto ou da própria contratada; V - reembolsar despesas com transporte, hospedagem e outros custos operacionais, que devem ser de exclusiva responsabilidade da contratada; VI - prever em edital exigências que constituam intervenção indevida da Administração na gestão interna dos fornecedores; VII - prever em edital exigência que os fornecedores apresentem, em seus quadros, funcionários capacitados ou certificados para o fornecimento da Solução, antes da contratação; VIII - adotar a métrica homem-hora ou equivalente para aferição de esforço, salvo mediante justificativa e sempre vinculada à entrega de produtos de acordo com prazos e qualidade previamente definidos; IX - contratar por postos de trabalho alocados, salvo os casos justificados mediante a comprovação obrigatória de resultados compatíveis com o posto previamente definido; e X - nas licitações do tipo técnica e preço: a) incluir critérios de pontuação técnica que não estejam diretamente relacionados com os requisitos da Solução de Tecnologia da Informação a ser contratada ou que frustrem o caráter competitivo do certame; e b) fixar os fatores de ponderação das propostas técnica e de preço sem justificativa, salvo quando o fator de ponderação for 50% (cinquenta por cento) para técnica e 50% (cinquenta por cento) para preço

B - RELAÇÃO ENTRE OS EVCR´s A NORMA ISO/IEC 27002:2013 E OS GUIAS DE MELHORES PRÁTICAS

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
Planejamento estratégico institucional e de TI	PO1.2 *Business-IT Alignment*			*SS* 2.1 *What is service management?* SS 2.3 *The business process* SS2.4 *Principles of service management*	
	PO1.4 *IT Strategic Plan*			SS 3.3 *Service provider types* SS 3.5 *Service strategy fundamentals* SS 4.1 *Define the market* SS 4.2 *Develop the offerings* SS 4.3 *Develop strategic assets* SS 4.4 *Prepare for execution* SS 5.5 *Demand management* SS 6.5 *Sourcing strategy*	
Política de Segurança	DS5.2 IT Security Plan (Plano de Segurança de TI) .			SS 5.2 *Return on investment* SS 5.3 *Service portfolio management* SS 5.4 Service portfolio management methods	Item 5 - Política de segurança da informação.

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
Comitê de Segurança da Informação ou Gestor de Segurança	PO4.3 *IT Steering Committee*				Item 6 - Responsabilidades e Papéis pela Segurança da Informação.
Gestão de Continuidade	DS4 Ensure Continuous Service (Garantir a Continuidade do Serviço)			SD 4.5 *IT service continuity management* SD 4.5.5.*1 Stage 1-Initiation* *CSI* 5.6.3 *IT Service continuity management* SD 4.5.5.2 *Stage* 2 *-Requirements and strategy* SD 4.5.5.3 *Stage 3 - Implementation* SD *App K The typical contents of a recovery plan* SD 4.4.5.2 *The proactive activities of availability management* SD 4.5.5.4 *Stage* 4 - *Ongoing operation* • SD 4.5.5.4 *Stage* 4*—Ongoing Operation*	17 – Aspetos de Segurança da Informação na Gestão de Continuidade do Negócio.
Classificação dos ativos de Informação	PO2.3 Data *Classification Scheme*			SD 5.2 Data and information Management	Item 8.2 – Classificação da Informação

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
Gestão de controle de acesso.	DS5.3 *Identity Management* (Gerência de Identidade).			SO 4.5 *Access management*	Item 9 – Controle de Acesso
	DS5.4 *User Account Management* (Gerência de Contas de Usuários)			SO 4.5 *Access management* • SO 4.5.5.1 *Requesting access* • SO 4.5.5.2 *Verification* • SO 4.5.5.3 *Providing rights* • SO 4.5.5.4 *Monitoring identity status* • SO 4.5.5.5 *Logging and tracking access* SO 4.5.5.6 *Removing or restricting rights*	Item 9 – Controle de Acesso
	DS12.2 *Physical Security Measures* (Medidas de Segurança Física).			*SO App E Detailed description of* facilities management	Item 11 – Segurança física e do Ambiente.
	DS12.3 *Physical Access* (Acesso Físico).			• *SO App E Detailed description of facilities management* • *SO App F Physical access control*	Item 11 – Segurança física e do Ambiente.

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
Gestão de incidentes	DS5.5 *Security Testing, Surveillance* and Monitoring (Teste, Vigilância e Monitoramento de Segurança - Testar e monitorar a implementação da segurança de TI de uma forma pró-ativa.			SO 4.5.5.6 *Removing or restricting* rights • SO 5.13 Information security management and service operation	Item 16 - Gestão de Incidentes de Segurança da Informação.
	DS5.6 *Security Incident Definition* (Definição de Incidente de Segurança - Definir e comunicar claramente as características de potenciais incidentes de segurança para que possam ser corretamente classificados e tratados pelo processo de gestão de problemas e de incidentes).			SD 4.6.5.1 Security controls (highlevel coverage, not in detail) • SD 4.6.5.2 Management of security breaches and incidents	

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
Processo de gestão de mudanças	*AI6 Manage Changes* (Gestão de Mudanças)			*SD 3.2 Balanced design* *• SD 3.7 The subsequent design activities* *• ST 3.2 Policies for service transition* *• ST 3.2.1 Define and implement a formal policy for service transition* *• ST 3.2.2 Implement all changes to services through service transition* *ST 3.2.7 Establish effective controls and disciplines* *ST 4.1 Transition planning and support* *ST 4.1.4 Policies, principles and basic concepts* *ST 4.2 Change management* *ST 4.2.6.1 Normal change procedure* *• ST 5 Service transition common operation activities* *• ST 6 Organising for service transition* *• ST 6.3 Organisation models to support service transition* *• ST 6.4 Service transition relationship with other life cycle*	Item 12.1.2 – Gestão de Mudanças.

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
				stages *• SO 4.6.1 Change management (as operational activities)* *ST 4.2.6.2 Create and record requests for change* *• ST 4.2.6.3 Review the request for change* *• ST 4.2.6.4 Assess and evaluate the change* *• ST 4.2.6.5 Authorising the change* *• ST 4.2.6.6 Co-ordinating change implementation* *• ST 4.2.6.8 Change advisory board* *• ST 4.6 Evaluation* *• SO 4.3.5.1 Menu selection* *• SO 4.3.5.2 Financial approval* *• SO 4.3.5.3 Other approval* *• ST 4.2.6.9 Emergency changes* *ST 3.2.13 Assure the quality of the new or changed service* *• ST 3.2.14 Proactively improve quality during service transition* *• ST 4.1.5.3 Planning and co-ordinating service transition* *• ST 4.1.6 Provide transition process support*	

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
				ST 4.2.6.4 Assess and evaluate the change *• ST 4.2.6.7 Review and close change record* *• ST 4.4.5.10 Review and close service transition* *• ST 4.4.5.9 Review and close a deployment* *• SO 4.3.5.5 Closure*	
Gestão de Riscos	PO9.4 Risk Assessment (Análise de Riscos)	*KA - Project Risk Management* *PG-Planning Process Group* *11.1 – Plan Risk Management* *11.2 – Identify Risks* *11.3 – Perform Qualitative Risk Analysis* *11.4 – Perfom Quantitative Risks Analysis* *11.5 – Plan Risk*	*PA - RSKM - Risk Management*	SS 9.5 *Risks* *• SD 4.5.5.2 Stage 2— Requirements and strategy* *• SD 8.1 Business impact analysis (not in detail)* *• ST 4.6 Evaluation*	Item 0.2 – Requisitos de Segurança da Informação.

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
		Responses *PG- Monitoring & Controlling Process Group* *11.6 Monitor and Controls Risks*			
Gestão de Ativos	PO2.2 - *Enterprise data dictionary and data syntax rules*		*CM - Configuration Manager*	SD 5.2 - *Data and information management* SD 7 - *Technology considerations*	Item 8 – Gestão de Ativos.
Gestão da Conformidade	PO 4.8 *Responsability for risk, security and compliance*.	SD 6.4 Roles and responsibilities.			Item 18 – Conformidade.
Gestão do uso de dispositivos móveis	PO 3.4 *Technology Standards*				Item 8 – Gestão de Ativos.
Gestão do uso de Tecnologias em Nuvem					Item 9 – Controle de Acesso

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
Gestão do uso de redes sociais					Item 9 – Controle de Acesso Item 13 – Segurança nas Comunicações.
Aquisição, Desenvolvimento de sistemas de informação	AI2.7 Development of *Application Software* (Desenvolvimento de Software Aplicativo).		*PROCESS AREAS:* *DAR - Decision Analysis and Resolution* *IPM - Integrated Project Management* *MA - Measurement and Analysis* *OPD - Organizational Process Definition* *OPF - Organizational Process Focus (OPF)* *OT - Organizational Training (OT)* *PI - Product Integration (PI)* *PMC - Project Monitoring and Control*	*SD 3.7.3 Develop the service solution*	14 - Aquisição, desenvolvimento e manutenção de sistemas de informação.

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
			PP - Projetc Planning *PPQA - Process and Product Quality Assurance (PPQA)* *RD - Requirements Development* *REQM - Requirements Management* *TS - Technical Solution* *VAL - Validation* *VER – Verification*		
Gestão de Acordos de Níveis de Serviço	DS1 Define and *Manage Service Levels* (Definir e Gerenciar Níveis de Serviço).		PA - SAM - *Supplier Agreement* Management	*SS 2.6 Functions and processes across the life cycle* *• SS 4.3 Develop strategic assets* *• SS 4.4 Prepare for execution* *• SS 7.2 Strategy and design* *• SS 7.3 Strategy and transitions* *• SS 7.5 Strategy and improvement* *• SD 4.2.5.1 Designing SLA frameworks* *• SD 4.2.5.9 Develop contracts and relationships*	12.4 – Registro e Monitoramento.

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
				SS 4.2 Develop the offerings *• SS 4.3 Develop strategic assets* *• SS 5.4 Service portfolio management methods* *• SS 5.5 Demand management* *• SS 7.2 Strategy and design* *• SS 7.3 Strategy and transitions* *• SS 7.4 Strategy and operations* *• SS 7.5 Strategy and improvement* *• SS 8.2 Service interfaces* *• SD 3 Service design principles* *• SD 3.1 Goals* *• SD 3.2 Balanced design* *• SD 3.4 Identifying and documenting business requirements and drivers* *• SD 3.5 Design activities* *• SD 3.6 Design aspects* *• SD 4.1 Service catalogue Management* *SD 4.2.5.2 Determine, document and agree upon requirements for new services and produce SLR* *• SD App F Sample SLA and operating level agreement (OLA)* *SD 4.2.5.5 Review and revise underpinning agreements and*	

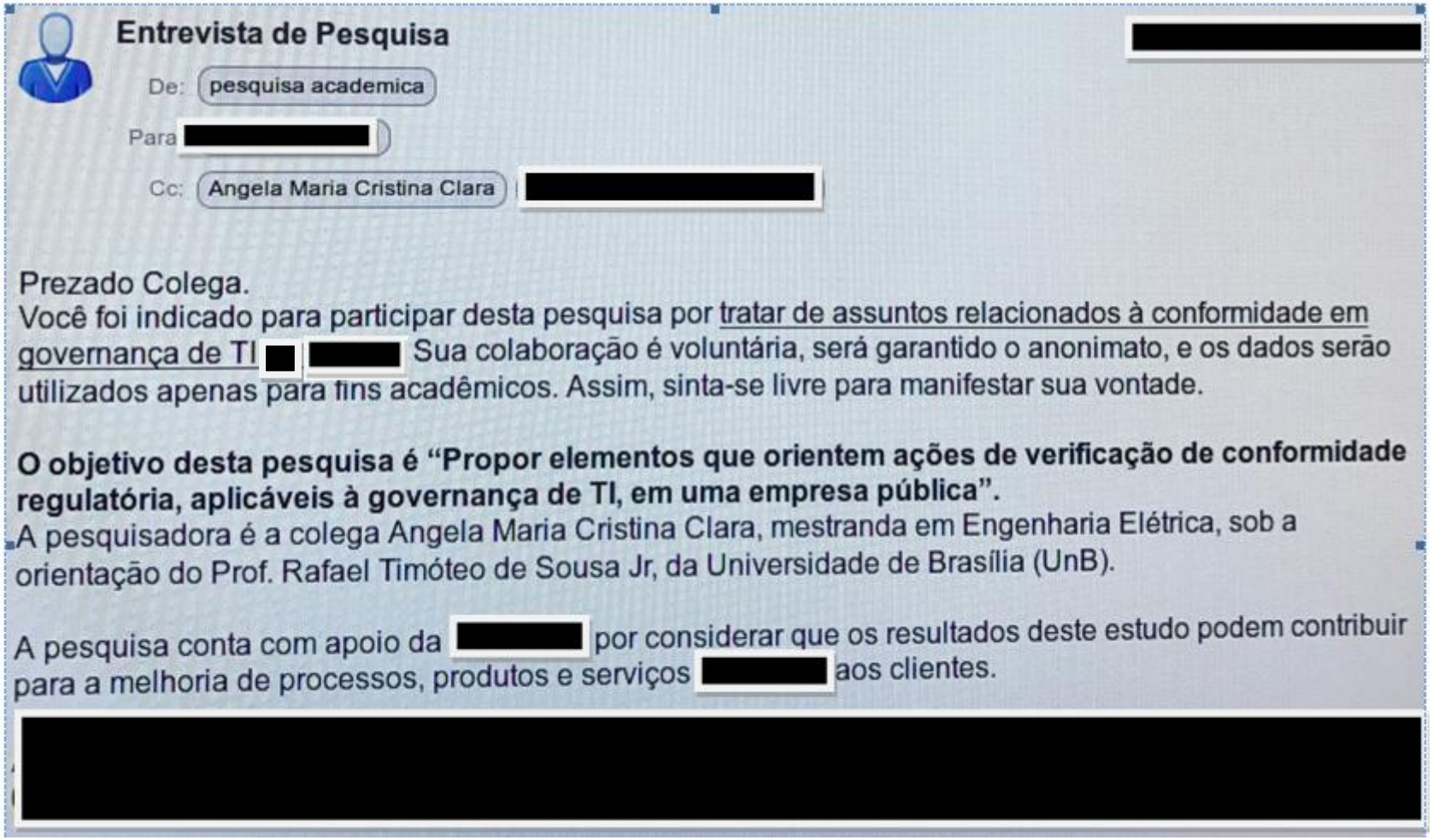
EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
				service scope *• SD App F Sample SLA and OL* *SS 5.3 Service portfolio management* *• SD 4.2.5.3 Monitor service performance against SLA* *• SD 4.2.5.6 Produce service reports* *• SD 4.2.5.7 Conduct service reviews* *and instigate improvements within an overall SIO* *• SD 4.2.5.10 Complaints and compliments* *• SD 4.3.8 Information management* *• CSI 4.2 Service reporting* *• CSI 4.3 Service measurement* *SD 4.2.5.4 Collate, measure and improve customer satisfaction* *• SD 4.2.5.5 Review and revise underpinning agreements and service scope* *• SD 4.2.5.8 Review and revise SLAs,* *service scope and underpinning*	

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
				agreements.	
Processo de contratação de bens e serviços de TI	AI5.1 Procurement Control (Controle sobre aquisições)			SD 3.7.2 Procurement of the preferred solution	14 - Aquisição, desenvolvimento e manutenção de sistemas de informação.
Processo de gestão de contratos de TI	AI5.1 Procurement Control (Controle sobre aquisições)			SD 3.7.2 Procurement of the preferred solution	15 – Relacionamento na Cadeia de Suprimentos.
	AI5.2 *Supplier Contract Management* (Gerenciamento de Contratos de Fornecedores).			• *SD 4.2.5.9 Develop contracts and relationships* • *SD 4.7.5.3 Establishing new suppliers and contracts.*	

EVCR´s	***COBIT*** **(I)**	**PMBOK - Quarta Edição** *(KA) Knowledge Areas* *(PG) Process Group* **(II)**	***CMMI* – Nível 3** ***Process Areas (PA)*** **(III)**	***ITIL* V3** (SS)– Estratégia de Serviço (SD) Desenho de Serviço (ST) Transição de Serviço (SO) Operação de Serviço (CSI) Melhoria Continuada do Serviço **(IV)**	**NORMA NBR/ISO/IEC 27002:2013** **(V)**
	DS2.2 *Supplier Relationship Management* (Gerenciamento de Relacionamento com Fornecedores)			SD 4.2.5.9 *Develop contracts and relationships* • *SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD)* • *SD 4.7.5.4 Supplier and contract management and performance* • *SD 4.7.5.5 Contract renewal and/or termination*	
	DS2.4 *Supplier Performance Monitoring (Monitoramento de Desempenho de Fornecedores).*			*SD 4.7.5.4 Supplier and contract management and performance*	

Fonte: autoria própria

C – PROCESSO DE APLICAÇÃO DE ENTREVISTA
C1 – CONVITE PARA REALIZAÇÃO DE ENTREVISTA



Entrevista de Pesquisa

[redacted]

De: pesquisa academica

Para [redacted]

Cc: Angela Maria Cristina Clara | [redacted]

Prezado Colega.
Você foi indicado para participar desta pesquisa por tratar de assuntos relacionados à conformidade em governança de TI [redacted] Sua colaboração é voluntária, será garantido o anonimato, e os dados serão utilizados apenas para fins acadêmicos. Assim, sinta-se livre para manifestar sua vontade.

O objetivo desta pesquisa é "Propor elementos que orientem ações de verificação de conformidade regulatória, aplicáveis à governança de TI, em uma empresa pública".
A pesquisadora é a colega Angela Maria Cristina Clara, mestranda em Engenharia Elétrica, sob a orientação do Prof. Rafael Timóteo de Sousa Jr, da Universidade de Brasília (UnB).

A pesquisa conta com apoio da [redacted] por considerar que os resultados deste estudo podem contribuir para a melhoria de processos, produtos e serviços [redacted] aos clientes.

[redacted]

C2 - ROTEIRO APLICADO NA REALIZAÇÃO DE ENTREVISTAS

ROTEIRO DE ENTREVISTA

Objetivo	Entrevistar empregados responsáveis pela Governança de TI da Empresa
Local	
Entrevistado	
Data de realização	
Horário	

1. Questões a serem respondidas pelo entrevistado

1. Como são definidas as estruturas, os papéis e as responsabilidades para atender a Governança de TI na Empresa?

2. Como se caracteriza o alinhamento da TI e o modelo de governança na Empresa?

3. Quais são as melhores práticas de TI aplicadas na Empresa e os respectivos processos organizacionais envolvidos? Cite exemplos.

4. Quais são os mecanismos aplicados na Empresa visando o alinhamento da TI com o negócio?

5. Quais são os métodos de medição de gestão de desempenho de TI aplicados na Empresa e os benefícios destes aos processos organizacionais?

6. Quais são os mecanismos aplicados na Empresa para promover uma cultura voltada a governança de TI? Cite exemplos.

7. Quais mecanismos são aplicados na empresa visando a agilidade e a qualidade dos processos de TI?

8. Quais são as principais ações (realizadas ou a realizar) para assegurar a efetividade do processo de gestão de riscos regulatórios e operacionais da TI na Empresa?

9. Quais são as ações realizadas na Empresa, relacionadas à governança de TI, que visam garantir a efetividade do processo de planejamento estratégico nos níveis estratégico, tático e operacional?

10. Quais são as ações realizadas na Empresa, visando a agilidade e qualidade dos processos de aquisição, desenvolvimento e manutenção de soluções?