FACULDADE DE TECNOLOGIA DE AMERICANA
Curso de Segurança da Informação

Stephanie Lissa Tsukamoto

ANÁLISE E GESTÃO DE RISCO PARA MITIGAR INCIDENTES DE SEGURANÇA

Americana, SP
2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso de Segurança da Informação

Stephanie Lissa Tsukamoto

ANÁLISE E GESTÃO DE RISCO COM RESPOSTA A INCIDENTES DE SEGURANÇA

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob a orientação da Professor Especialista Edson Roberto Gaseta.

Americana, SP

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

T819a TSUKAMOTO, Stephanie Lissa
Análise e gestão de risco para mitigar incidentes de segurança. / Stephanie Lissa Tsukamoto. – Americana: 2016.
91f..

Monografia (Curso de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Edson Roberto Gaseta

1. Segurança em sistemas de informação I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Stephanie Lissa Tsukamoto

ANÁLISE E GESTÃO DE RISCO PARA MITIGAR INCIDENTES DE SEGURANÇA

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 09 de Dezembro de 2016.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
Fatec Americana

Pedro Domingos Antoniolli (Membro)
Doutor
Fatec Americana

Leandro Halle Najm (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar agradeço aos meus pais pelo apoio durante o curso, aos meus amigos que estiveram ao meu lado durante a trajetória, e aos professores que fizeram despertar a paixão pela área.

DEDICATÓRIA

A minha família.

RESUMO

O presente documento conceitua o que é análise e gestão de risco, que é avaliação dos potenciais problemas que podem ocorrer dentro da empresa, seguindo com a explicação sobre o que é risco, e assim conceituar sobre o que são vulnerabilidades e ameaças para a organização. Neste trabalho de conclusão de curso é explicado brevemente sobre plano de continuidade de negócio, que serve para garantir uma ação planejada com antecedência quando acontecer um desastre e o que é necessário para manter os serviços básicos da empresa. Explica brevemente sobre governança de tecnologia da informação e ciclo de análise, onde este informa sobre a análise dos riscos. Neste documento, também adentra e explica sobre métodos para verificar a maturidade do negócio, como a ISO 27005 que fornece um modelo para melhorar um Sistema de Gestão de Segurança da Informação, mas é focado no COBIT, principalmente nos processos PO9, AI6, AI7, DS5 e DS8, estes sendo os mais relevantes para a pesquisa e análise. Neste artigo também é brevemente explicado para fins acadêmicos sobre o COBIT 5. Introduzir-se sobre resposta a incidentes que é responsável por trazer os procedimentos do que deve ser feito caso alguma vulnerabilidade torne-se real. E por fim, é documentado o estudo de caso utilizando o método de identificar o nível de maturidade do negócio, de acordo com alguns times de suporte nível 1 (*Mainframe*, Redes e Sistemas Distribuídos) e nível 2 (Banco de Dados), utilizando alguns processos do COBIT 4.1. Desta forma, pode-se identificar diferenças entre alguns times, e verificar quais as deficiências que estes apresentam, e criar sugestões para poder alcançar o mais alto nível de maturidade com base no COBIT 4.1.

[E1] Comentário: O resumo está muito pequeno, necessário colocar mais informações

Palavras Chave: COBIT, Incidente, Risco, Plano de Continuidade do Negócio.

ABSTRACT

This document conceptualizes what analysis and risk management and is, it is the evaluation of potential problems that can occur within the company, following the explanation about risk, and then conceptualize what are the vulnerabilities and threats to the organization. In this monograph is briefly explained about business continuity plan, which serves to ensure action when disaster strikes and what is necessary to maintain basic services for the company. It briefly explains governance of information technology and analysis cycle, where it informs about risk analysis. In this document, it also introduces and explains methods for verifying business maturity, such as ISO 27005, which provides a model for improving an Information Security Management System, but focuses on COBIT, mainly in processes PO9, AI6, AI7, DS5 and DS8, these being the most relevant for research and analysis. This document is also briefly explained for academic purposes on COBIT 5. Introduce on incident response which is responsible for bringing the proceedings of what should be done when some vulnerability become real. Finally, the case study is documented using the method of identifying the level of business maturity, according to some support teams level 1 (Mainframe, Networks and Distributed Systems) and level 2 (Database), using some COBIT 4.1 processes, in this way, it is possible to identify differences between some teams and to check the deficiencies they present and to create suggestions to reach the highest level of maturity based on COBIT 4.1

Keywords: *COBIT, Incident, Risk, Business Continuity Plan.*

SUMÁRIO

LISTA DE FIGURAS E DE TABELAS

1 INTRODUÇÃO

Neste documento, foi verificado e introduzido conceitos sobre análise e gestão de riscos, com definições sobre o ameaças e vulnerabilidades, assim como introdução as metodologias COBIT 4.1 e a ISO 27005.

Para isso foi pesquisado o que é risco de segurança da informação e como analisar uma vulnerabilidade, além de pesquisar sobre plano de resposta a incidentes de segurança da informação e a organização para qual são reportados os casos de incidentes de segurança. Além de alguns tipos de *frameworks*[1] utilizados para realizar a governança de Tecnologia da Informação.

Esse trabalho teve como objetivo geral a análise de um processo de plano de resposta a incidentes de uma organização.

A metodologia de pesquisa utilizada foi a científica com caráter bibliográfico, que segundo Marconi e Lakatos (1992) é o levantamento de toda bibliografia já publicada como livros, artigos, teses e dissertações que contém o método quantitativo que busca conceituar os temas e princípios propostos nesse trabalho, com foco na utilização do COBIT 4.1.

Além da pesquisa de campo que de acordo com Marconi e Lakatos (1992) é a forma de levantamento de dados em um local, ou diversos locais em que ocorrem o problema proposto.

O trabalho foi estruturado em três capítulos, sendo que o primeiro conceitua o que é risco e conceitos teóricos sobre a análise e gestão de riscos, o que é e como realizar um plano de resposta a incidentes de segurança, as ferramentas mais utilizadas para fazer um plano de continuidade de negócio, a análise de um plano de continuidade de negócio, no terceiro sendo o estudo de caso e por último as conclusões obtidas através desse estudo.

[1] Ferramentas

2 ANÁLISE E GESTÃO DE RISCOS

Quando se trabalha com a questão de análise e gestão de riscos e respostas a incidentes é necessário conceituar o que é risco.

Segundo Westerman e Hunter (2008, p.01), risco "é a possibilidade de algum evento imprevisto que envolva falha ou mau uso da TI, ameaça um objetivo empresarial".

La Rocque (2007, p.12) definiu risco como:

> O risco é inerente a qualquer atividade na vida pessoal, profissional ou nas organizações, e pode envolver perdas, bem como oportunidades. Em finanças, a relação risco-retorno indica que quanto maior o nível de risco aceito, maior o retorno esperado dos investimentos. Esta relação vale tanto para investimentos financeiros como para os negócios cujo "retorno" é determinado pelos dividendos e pelo aumento do valor econômico da organização.

Já a FENACOR (2011) conceitua risco um "evento incerto ou de data incerta que independe da vontade das partes contratantes".

Sendo assim, o risco é a possibilidade de um evento que não pode ser previsto acontecer, podendo ser na área de TI (Tecnologia da Informação) ou não, mas o fator é conhecido e pode ser minimizado. O risco pode ser a combinação da ameaça com as vulnerabilidades (fraquezas) identificadas.

A análise e gestão de risco faz uma avaliação dos potenciais incidentes que podem ocorrer dentro da empresa, verificando possíveis vulnerabilidades que podem expor o empreendimento. Neste trabalho o tema está na área de tecnologia da informação.

O conceito de gerência de risco, de acordo com Cendrowski e Mair (2001, p.05):

> A gestão de riscos corporativos é um processo efetuado pelo conselho de administração de uma entidade, sua direção e todo o pessoal, aplicável à definição de estratégias em toda a empresa e desenhado para identificar eventos potenciais que podem afetar a organização, gerir seus riscos dentro do risco aceito e proporcionar uma segurança razoável sobre o alcance dos objetivos.

Segundo a ISO[2] (2016) todas as atividades de uma empresa envolvem risco, assim gerenciam os riscos identificando e analisando o risco e assim avaliando o que deve ser feito.

---

[2] *International Standard Organization*: Organização Internacional para Padronização

Outra questão para a organização tornar efetiva a melhoria do tratamento dos riscos e diminuição dos riscos é a continuidade das análises de risco, assim a ISO recomenda que deva haver um ciclo de análise dos riscos.

A análise e gerenciamento de riscos pela ISO são atividades que devem ser averiguados junto com os *stakeholders*[3], depois monitorados e revistos para que deste modo sejam verificadas quais ações devem ser tomadas.

Segundo Picolini e Bezerra (2015), para iniciar a análise de risco, de princípio são listados os processos que ocorrem na empresa. Depois é feito uma análise quantitativa e qualitativa dos bens da empresa, buscando estimar os custos associados a cada recurso.

Deste modo, Bezerra (2015) define que ameaças são eventos que podem explorar as vulnerabilidades, sendo um potencial para resultar em um dano ao sistema ou organização. As vulnerabilidades são fraquezas que podem ser exploradas pelas ameaças, o que pode gerar um impacto para toda a empresa, considerando estes pontos a serem analisados:

- Os riscos de segurança da informação, que é a possibilidade de uma ameaça explorar uma vulnerabilidade.
- Identificação de riscos, processos para localizar, listar e caracterizar elementos de risco.
- O impacto que pode causar a empresa caso uma dessas vulnerabilidades se torne real. O impacto pode ser uma mudança adversa no nível obtido dos objetivos do negócio.

Um fator de difícil análise são as pessoas envolvidas, pessoas que atuam diretamente no sistema, afetam diretamente na qualidade de serviço prestado. Falta de treinamento ou qualificação pode trazer riscos, intencionais ou não. Uma pessoa não qualificada ou treinada adequadamente pode causar danos em qualquer intenção, resultado de omissão ou negligência por parte dela. Já o caso de intenção, ela pode ser a causa de desaparecimento de equipamentos como também a causa de falha de um sistema, por desligar propositalmente um equipamento essencial para o funcionamento da companhia.

[3] Partes interessadas no negócio.

O risco em cima dos sistemas são aqueles oriundos de falha de equipamento, problema de rede, manutenção ineficiente, queda de energia por meio externo, assim como lentidão do sistema.

Outros fatores a serem analisados, mas sem que a organização tenha controle sobre são, catástrofes naturais, vandalismo e interrupção de serviços públicos.

Bezerra (2015) utiliza a ISO 27005 para fazer a análise e gerenciamento dos riscos desta forma, verificando com a organização possíveis ações para tratar as vulnerabilidades das quais ela está disposta investir ou a aceitar os riscos devido ao fato da disponibilidade financeira que esta possui para cada problema, entrando assim na relação entre o custo X benefício.

Se para a empresa, alguma vulnerabilidade não impactará de forma significativa e trará um custo de tratamento muito alto, ela poderá aceitar aquele risco.

Para poder fazer uma aceitação do risco mais segura, deve se analisar com base na lista de vulnerabilidades e ameaças o valor de cada ativo, tanto financeiro como valor relativo.

O valor financeiro é o valor que foi efetivamente gasto em um equipamento, levando em conta o custo da implantação do sistema. O valor relativo é o quanto pode se perder quando um equipamento ou rede para de funcionar, assim sendo o quanto a empresa pode perder caso o sistema está fora de funcionamento.

E por fim, para determinar a aceitação do risco, existe um cálculo baseado nas vulnerabilidades, ameaças, valor, probabilidade e impacto, assim tendo uma base para definir o que a empresa pode mesmo aceitar e quais vulnerabilidades terá que tomar providências para não criar um prejuízo para a empresa e seus clientes.

Segundo Westerman e Hunter (2008, p.01) “um incidente de risco de TI tem o potencial de gerar consequências comerciais que afetam uma vasta gama de stakeholders”

Depois de uma análise, cálculo e aceitação de riscos, a empresa deverá criar uma resposta para cada incidente causado por possíveis vulnerabilidades existentes, criando um procedimento de ações a serem tomadas. Para tal, deve-se utilizar a resposta a incidentes.

2.1 CICLO DE ANÁLISE

O risco precisa ser avaliado pela organização, para Cendrowski e Mair (2009 p.4):

> O processo de avaliação do risco consiste de 5 etapas: A enumeração dos riscos, a análise qualitativa, a análise quantitativa, a estratégia de implantação de gerenciamento de risco e a avaliação estratégica do gerenciamento risco.

- Enumeração dos riscos: deve-se ao objetivo de levantar todos os fatores, atividades e processos internos da empresa e verificar qual são os riscos da organização;
- Análise qualitativa: refere-se ao fato de saber desses riscos apontados para que os gestores possam começar a definir estratégias;
- Análise quantitativa: refere-se a determinar valores do grau de risco de cada atividade dentro de uma empresa;
- Estratégia de implantação de gerenciamento de riscos: é quando os gestores de cada setor apresentam as estratégias para minimizar os riscos;
- Avaliação estratégica do gerenciamento de risco: é a renovação e ajustes das estratégias estabelecidas, assim o plano sempre está atualizado e cobrindo as falhas que forem detectadas.

2.2 PLANO DE CONTINUIDADE DE NEGÓCIO

O PCN[4] (*Business Continuity Plan*) teve a sua norma estabelecida pela ABNT 15.999 (2002, p.7) Parte 1 até 05/10/2015, e tinha como objetivo entender, desenvolver, implementar um PCN na organização, além de fornecer segurança para os clientes e outras empresas, ela permite a avaliação de um plano de continuidade de negócio de forma reconhecida.

Ela foi substituída pela ABNT (2002) que tem como objetivo fornecer orientação para o planejamento, criação, prática, monitoramento, análise e mensuração de forma contínua e documentada. Essa norma permite que as empresas se preparem para responder e se recuperar de incidentes.

[4] Plano de Continuidade de Negócio

O plano de continuidade de negócio serve para garantir uma ação quando acontecer um desastre e é necessário manter os serviços básicos da empresa.

O PCN divide o funcionamento da empresa em duas partes:

- Componentes: são as variáveis utilizadas pelo processo, são elas, T.I., energia, pessoas, espaço, tempo, estrutura-física.
- Processos: são as atividades da empresa.

2.3 GOVERNANÇA DE TI

A governança de TI para Tomiatti (2012, p.15, apud. IGTI) "é de responsabilidade da diretoria e gerência executiva e que a governança de TI faz parte da governança da empresa".

De acordo com Weill (2006) "Governança de TI: a especificação dos direitos decisórios e do framework de responsabilidades para estimular comportamentos desejáveis na utilização da T.I. "

> Governança de TI é de responsabilidade do Corpo de Diretores e Gerencial. GTI integra a Governança da Empresa e consiste em mecanismos de liderança, estrutura organizacional e processos e garantem que a TI da organização mantém e alcançam a s estratégias e objetivos da organização. Tomiatti (2012, p.16, apud. BOARD BRIEFING ON IT GOVERNANCE).

A governança possui *frameworks*[5] e modelos de boas práticas que auxiliam a empresa a alinha a TI à estratégia da empresa, no caso do plano de continuidade de negócio e resposta a incidentes, dois *frameworks* se destacam: ISO 27005 e COBIT 5.

2.3.1 COBIT 4.1

O COBIT[6] (Control Objectives for Information and related Technology):

> fornece boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável. As boas

[5] Ferramentas
[6] Objetivos de Controle para a Informação e tecnologia

> práticas do COBIT representam o consenso de especialistas. Elas são fortemente focadas mais nos controles e menos na execução. Essas práticas irão ajudar a otimizar os investimentos em TI, assegurar a entrega dos serviços e prover métricas para julgar quando as coisas saem erradas. (IT Governance Institute. COBIT 4.1)

Foi desenvolvido pela ISACA (Information System Audit and Control Association), é um *framework* que permite a visão da importância da TI para a organização.

Para Tomiatti (2012, p.20, apud. Caciato) o COBIT 4.1 baseia sua estrutura em indicadores de performance que permite monitorar o quanto a TI agrega valor ao negócio.

> A metodologia COBIT consiste em objetivos de negócio ligados a objetivos de TI, provendo métrica s e modelos de maturidade para medir sua eficácia e identificando as responsabilidades relacionadas dos donos dos processos de negócios e de TI. Tomiatti (2012, p.20, apud. IT GOVERNANCE INSTITUTE)

O COBIT 4.1 possui quatro domínios, que para Tomiatti (2012, p. 21) são eles:

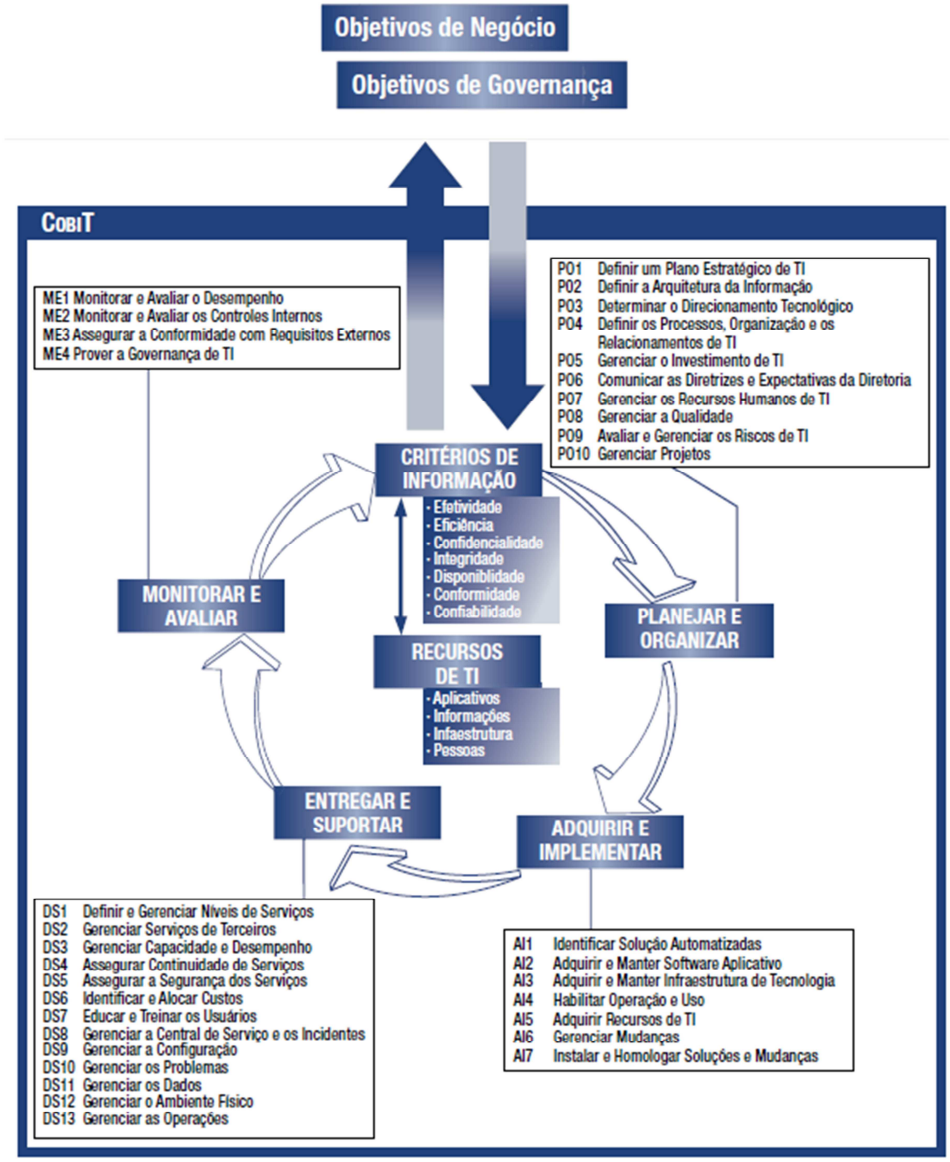
> Planejar e Organizar (PO): provê direção de entrega de soluções (AI) e serviços (DS); - Adquirir e Implementar (AI) - provê as soluções e a s transfere para tornarem-se serviços; - Entregar e Suportar (DS): recebe a s soluções e as torna passíveis de uso pelos usuários finais; - Monitorar e Avaliar (ME): monitora todos os processos para garantir que a direção definida seja seguida.

E essas práticas fornecem uma ferramenta para gerenciar os serviços de TI, esse modelo promove o gerenciamento com foco na qualidade dos serviços de TI para o cliente.

O COBIT 4.1, possui uma estrutura com vários processos, das quais fazem com que tenha um ciclo de análise, começando por processos de monitoração e análise (processos iniciando do ME1 ao ME4), seguindo para o processo de planejamento e organização (processos começando pelo PO1 ao PO10), seguido pelos processos de adquirir e implementar (processos do AI1 ao AI7) e finalmente terminando nos processos de entrega e suporte (processos DS1 ao DS13).

Sendo melhor explicado e detalhado na figura à seguir:

Figura 1: Visão geral COBIT 4.1



Fonte: IT Governance Institute (2007).

Para este trabalho será focado nos processos PO9, AI6, AI7, DS5 e DS8, pois estes processos satisfazem as necessidades de negocio, com todas as etapas possuindo processos de avaliação e cálculos de maturidade da empresa, sendo eles detalhados a seguir.

2.3.1.1 Processo PO9 para analisar e gerenciar os Riscos de TI

O processo PO9 tem o objetivo de criar e manter uma estrutura de gestão de risco, segundo o IT Governance Institute (2007):

> Esta estrutura documenta um nível comum e acordado de riscos de TI, estratégias de mitigação e riscos residuais. Qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado. Estratégias de mitigação de risco devem ser adotadas para minimizar o risco residual a níveis aceitáveis. O resultado da avaliação deve ser entendido pelas partes interessadas e expresso em termos financeiros para permitir que as partes interessadas alinhem o risco a níveis de tolerância aceitáveis.

Para o IT Governance Institute (2007), esta etapa tem como objetivo analisar e comunicar os riscos de TI e possíveis impactos nos processos e objetivos de negócio, com foco em desenvolver uma estrutura de gerenciamento de risco integrada as estruturas corporativas e operacionais de gerenciamento de risco, avaliação, mitigação e comunicação de risco residual.

Sendo alcançado por uma garantia de que o gerenciamento de risco esteja completamente integrado aos processos gerenciais, interna e externamente, e seja aplicado de forma consistente com a realização de avaliações de risco, recomendação e comunicação de planos de ações de remediações dos riscos, sendo medidos por percentual de objetivos críticos de TI, cobertos pela avaliação de riscos, percentual de riscos críticos de TI, identificados que tenham planos de ação desenvolvidos e percentual dos planos de ação de gestão de riscos aprovados pela implementação.

O PO9 possui alguns critérios de avaliação e assim são criadas questões para que possa haver respostas para calcular o nível de maturidade da empresa, o IT Governance Institute utiliza os seguintes tópicos para a avaliação:

> - **PO9.1 Alinhamento da gestão de riscos de TI e de Negócios:** Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).
> - **PO9.2 Estabelecimento do Contexto de Risco:** Estabelecer o contexto ao qual a estrutura de avaliação de risco é aplicada para assegurar resultados esperados. Isso inclui a definição dos contextos interno e externo de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos são avaliados.

- **PO9.3 Identificação de Eventos:** Identificar eventos (importante ameaça real que explora significativas vulnerabilidades) com potencial impacto negativo nos objetivos ou nas operações da organização, incluindo aspectos de negócios, regulamentação, aspectos jurídicos, tecnologia, parcerias de negócio, recursos humanos e operacionais. Determinar a natureza do impacto e manter esta informação. Registrar e manter um histórico dos riscos relevantes.
- **PO9.4 Avaliação de Risco:** Avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos. A probabilidade e o impacto associado ao risco inerente e residual devem ser determinados individualmente, por categoria e com base no portfólio da organização.
- **PO9.5 Resposta ao Risco:** Desenvolver e manter um processo de respostas a riscos para assegurar que controles com uma adequada relação custo-benefício mitiguem a exposição aos riscos de forma contínua. O processo de resposta ao risco deve identificar estratégias de risco, tais como evitar, reduzir, compartilhar ou aceitar o risco, determinar responsabilidades, e considerar os níveis de tolerância definidos.
- **PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco:** Priorizar e planejar as atividades de controle em todos os níveis da organização para implementar as respostas aos riscos identificadas como necessárias, incluindo a identificação de custos, benefícios e responsabilidade pela execução. Obter aprovações para ações recomendadas e aceitação de quaisquer riscos residuais e assegurar que as ações aprovadas sejam assumidas pelos donos dos processos afetados. Monitorar a execução dos planos e reportar qualquer desvio para a Alta Direção.

2.3.1.2 Processo AI6 para Gerenciar Mudanças

Esta etapa é responsável por todas as mudanças, manutenções e correções, emergenciais ou não que são relacionadas a infraestrutura e aplicação no ambiente corporativo. Essas mudanças como procedimentos, processos, parâmetros de sistemas e de serviço devem ser registradas, avaliadas e autorizadas antes da implementação e ser revisadas assim que completadas, para assegurar a mitigação dos riscos de impacto negativo na estabilidade ou integridade do ambiente.

Segundo o IT Governance Institute (2007) este tem com foco, fazer o controle das avaliações de impacto, autorização e implementação das mudanças de infraestrutura, aplicações e soluções técnicas de TI. Minimizando os erros com requisitos específicos incompletos e interromper a implementação não autorizada, e este é alcançado por definições e comunicação de procedimentos de mudanças que incluem mudanças emergenciais, avaliando, priorizando e autorizando mudanças, e fazer o acompanhamento de status e apresentação de relatório de mudanças. E medido por fim pela quantidade de paradas ou erros devido a especificações inadequadas ou avaliação de impacto critico incompletas, assim como o retrabalho

de infraestrutura ou aplicação causado por especificações de mudança inadequada. Também com o cálculo de percentual de mudanças que seguem o processo formal de controle de mudanças.

Os processos de análise para gestão de mudanças estão no tópico a seguir:

- **AI6.1 Padrões e Procedimentos de Mudança:** Estabelecer procedimentos formais de gerenciamento de mudanças para lidar de modo padronizado com todas as solicitações de mudança em aplicações, procedimentos, processos, parâmetros de sistema, parâmetros de serviço e plataformas subjacentes (inclusive solicitações de manutenção e reparo).
- **AI6.2 Avaliação de Impacto, Priorização e Autorização:** Avaliar todas as solicitações de mudança de modo estruturado com relação a impactos no sistema operacional e na respectiva funcionalidade. Assegurar que todas as mudanças sejam categorizadas, priorizadas e autorizadas.
- **AI6.3 Mudanças de Emergência:** Estabelecer um processo para definição, solicitação, testes, documentação, avaliação e autorização de mudanças de emergência que não sigam o processo de mudança estabelecido.
- **AI6.4 Acompanhamento de Status e Relatórios de Mudanças:** Estabelecer um sistema de acompanhamento e relatórios de mudanças para documentar mudanças rejeitadas, comunicar o status de mudanças aprovadas e em andamento e executar mudanças. Garantir que as mudanças autorizadas sejam implementadas conforme planejado.
- **AI6.5 Finalização da Mudança e Documentação:** Atualizar a documentação os procedimentos do sistema e de usuários sempre que forem implementadas mudanças no sistema

2.3.1.3 Processo AI7 para Instalar e Homologar Soluções de Mudanças

Nesta etapa, é descrito pelo IT Governance Institute (2007) para que haja a implementação de sistemas novos, já testados e com o desenvolvimento concluído, é necessário que sejam feitos testes em um ambiente dedicado, com dados de testes relevantes, definição de implantação e migração, planejamento e liberação e mudanças no ambiente de produção e uma revisão pós-implementação, com isso assegura se que os sistemas operacionais estejam alinhados com as expectativas e os resultados acordados.

O IT Governance Institute (2007) informa que para que haja a satisfação do cliente, é necessário que não ocorra nenhum problema após a implantação do sistema ou equipamento novo. Este também possui o foco em testar as aplicações e soluções de infraestrutura que atendam ao proposito pretendido, livres de erros e planejar e implementar e migrar para a produção.

Para que isso ocorra, é necessário que seja estabelecido uma metodologia de testes, realizar planejamento de liberação para produção, avaliar e aprovar resultados de testes pelos responsáveis e a realização de revisões após implementação, e este é medido pelo tempo de indisponibilidade da aplicação ou pela quantidade de correções dados devido a testes inadequados, percentual de sistemas que na avaliação pós-implementação alcança os benefícios planejados inicialmente e o percentual de projetos que tenham o plano de testes documentados e aprovados.

Para isso é necessário que seja avaliado com os tópicos a seguir, como sugerido pelo IT Governance Institute (2007):

- **AI7.1 Treinamento:** Treinar a equipe dos departamentos usuários envolvidos e as equipes de operações de TI de acordo com o plano de implementação e treinamento definido e os materiais associados, como parte de todos os projetos de desenvolvimento, implementação ou modificação de sistemas de informação.
- **AI7.2 Plano de Teste:** Estabelecer um plano de teste baseado nos padrões organizacionais que definem papéis, responsabilidades e critérios de sucesso de entrada e saída. Assegurar que o plano seja aprovado pelas partes relevantes.
- **AI7.3 Plano de Implementação:** Estabelecer um plano de implementação e de retorno à configuração anterior. Obter aprovação de todas as partes relevantes.
- **AI7.4 Ambiente de Testes:** Estabelecer um ambiente de testes seguro que reflita o ambiente de operações planejado no que diz respeito a segurança, controles internos, práticas operacionais, exigências de qualidade e confidencialidade e cargas de trabalho.
- **AI7.5 Conversão de Dados e Sistemas:** Planejar a conversão de dados e a migração da infraestrutura como parte dos métodos de desenvolvimento da organização, incluindo trilhas de auditoria, procedimentos de retorno à situação anterior e de recuperação de falhas.
- **AI7.6 Teste de Mudanças:** Assegurar que as mudanças sejam testadas de maneira independente e de acordo com o plano de testes definido antes da migração para o ambiente de produção.
- **AI7.7 Teste de Aceitação Final:** Assegurar que o gerenciamento do departamento usuário e da área de TI avalie o resultado do processo de testes como determinado no plano de testes. Corrigir erros significativos identificados no processo de testes, executar todos os testes listados no plano de testes, bem como qualquer teste de regressão necessário. Após a avaliação, aprovar a promoção para a produção.
- **AI7.8 Promoção para a Produção:** Após a conclusão dos testes, controlar a transferência dos sistemas alterados para operação, de acordo com o plano de implementação. Obter a aprovação das partes interessadas, como usuários, proprietário do sistema e gerência operacional. Quando apropriado, executar o sistema em paralelo com o sistema antigo durante um período e comparar comportamento/resultados.
- **AI7.9 Revisão pós-implementação:** Estabelecer procedimentos em linha com o gerenciamento de mudanças organizacionais para garantir a realização da revisão pós-implementação, conforme definido no plano de implementação.

2.3.1.4 Processo DS5 para Garantir a Segurança dos Sistemas

O IT Governance Institute (2007) define que nesta etapa deve-se manter a integridade da informação, protegendo os ativos de TI, implementando um processo de gestão de segurança, isto inclui o estabelecimento e a manutenção de papeis, responsabilidades, politicas, padrões e procedimentos de segurança.

Nisso também se incluem o monitoramento, teste periódico e a implementação de ações corretivas das deficiências, ou dos incidentes de segurança, uma gestão de segurança eficaz protege todos os ativos de TI e minimiza os impactos sobre o negócio.

Esta etapa também tem o foco de definir políticas, procedimentos e padrões de segurança, monitorar, detectar, reportar e solucionar vulnerabilidades e incidentes de segurança. Para que isso seja alcançado, é necessário que entenda-se os requisitos, vulnerabilidades e ameaças de segurança, gerenciando de forma padronizada as identidades e autorizações de usuários, assim como testes periódicos de segurança, e isso é medido pela quantidade de incidentes que prejudicam a reputação pública da corporação, quantidade de sistemas em que os requisitos de segurança não são atendidos e também pela quantidade de violações na segregação de funções.

Segundo o IT Governance Institute (2007), é necessário que essas análises sejam feitas:

> - **DS5.1 Gestão da Segurança de TI:** Gerenciar a segurança de TI no mais alto nível organizacional da empresa de modo que a gestão das ações de segurança esteja em alinhamento com os requisitos de negócio.
> - **DS5.2 Plano de Segurança de TI:** Traduzir os requisitos de negócio, de risco e conformidade, em um plano abrangente de segurança de TI, que leve em consideração a infraestrutura de TI e a cultura de segurança. O plano deve ser implementado em políticas e procedimentos de segurança, juntamente com investimentos adequados em serviços, pessoal, software e hardware. Políticas e procedimentos de segurança devem ser comunicados aos usuários e partes interessadas.
> - **DS5.3 Gestão de Identidade:** Todos os usuários (internos, externos e temporários) e suas atividades nos sistemas de TI (aplicação de negócio, desenvolvimento, operação e manutenção de sistemas) devem ser identificáveis de modo exclusivo. Os direitos de acesso dos usuários aos sistemas e dados devem estar em conformidade com as necessidades dos negócios e com os requisitos da função definidos e documentados. Os direitos de acesso devem ser solicitados pela gestão de usuários, aprovados pelo proprietário do sistema e implementados pelo responsável pela segurança. As identidades e os direitos de acesso dos usuários devem ser mantidos em um repositório central. É necessário implementar e manter atualizadas medidas técnicas e de procedimentos com boa relação custo-

benefício para determinar a identificação dos usuários, implementar a devida autenticação e impor direitos de acesso.

- **DS5.4 Gestão de Contas de Usuário:** Assegurar que a solicitação, a emissão, a suspensão, a modificação e o bloqueio de contas de usuário e dos respectivos privilégios sejam tratados por procedimentos de gestão de contas de usuário. Incluir um procedimento de aprovação de concessão de direitos de acesso pelos proprietários dos dados ou sistemas. Esse procedimento deve ser aplicado a todos os usuários, inclusive aos administradores (usuários com privilégios), usuários internos e externos, para os casos normais ou emergenciais. Os direitos e obrigações relativos ao acesso a sistemas e informações corporativos devem ser definidos em contrato para todos os tipos de usuários. Devem ser feitas revisões frequentes de todas as contas e os respectivos privilégios.
- **DS5.5 Teste de Segurança, Vigilância e Monitoramento:** Garantir que a implementação de segurança de TI seja testada e monitorada proativamente. A segurança de TI deve ser revalidada periodicamente para garantir que o nível de segurança aprovado seja mantido. A função de monitoramento e registro de eventos *(logging)* deve possibilitar a prevenção e/ou detecção prematura de atividades anormais e incomuns que precisem ser tratadas, bem como a subsequente geração de relatórios no tempo apropriado.
- **DS5.6 Definição de Incidente de Segurança:** Definir e comunicar claramente as características de incidentes de segurança em potencial para que possam ser tratados adequadamente pelos processos de gestão de incidentes ou gestão de problemas.
- **DS5.7 Proteção da Tecnologia de Segurança:** Garantir que as tecnologias de segurança importantes sejam invioláveis e que as documentações de segurança não sejam reveladas desnecessariamente.
- **DS5.8 Gestão de Chave Criptográfica:** Assegurar que sejam estabelecidos políticas e procedimentos de geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, uso e arquivamento das chaves criptográficas visando proteger contra sua modificação ou revelação pública não autorizada.
- **DS5.9 Prevenção, Detecção e Correção de Software Malicioso:** Assegurar que medidas preventivas, de detecção e corretivas sejam estabelecidas corporativamente, em especial correções de segurança *(patches)* e controles de vírus, para proteger os sistemas de informação e tecnologias contra malwares (vírus, *worms, spyware, spam.).*
- **DS5.10 Segurança de Rede:** Garantir que técnicas de segurança e procedimentos de gestão relacionados (como *firewalls*, aplicativos de segurança, segmentação de rede e detecção de intrusão) sejam utilizados para autorizar o acesso e controlar os fluxos de informação entre redes.
- **DS5.11 Comunicação de Dados Confidenciais:** Assegurar que as transações de comunicação de dados confidenciais ocorram somente por um caminho confiável ou controlado de modo a fornecer autenticação de conteúdo, comprovante de envio, comprovante de recebimento e não-rejeição de origem

2.3.2.5 Processo DS8 para Gerenciar a Central de Serviços e os Incidentes

Para esta etapa, segundo o IT Governance Institute é necessário que haja uma central de serviços para que a resposta seja efetiva e em tempo adequado, assim como processos de gerenciamento de incidentes sejam bem projetados e

implementados, isto inclui implementação de uma central de serviços capacitada para o tratamento de incidentes, incluindo registro, encaminhamento, análise de tendência, análise da causa-raiz e resolução, com isso a empresa é beneficiada com o aumento de produtividade por meio de resolução rápida dos chamados.

Para fazer a análise desta etapa, o IT Governance Institute (2007) sugere:

> - **DS8.1 Central de Serviço:** Estabelecer uma central de serviço, que é a interface entre o usuário e a TI, para registrar, comunicar, despachar e analisar todos os chamados, incidentes reportados, solicitações de serviços e demanda de informações. Devem existir procedimentos de monitoramento e encaminhamento com base em níveis de serviço acordados relativos ao SLA adequado que permita a classificação e a priorização de qualquer dúvida reportada como incidente, solicitação de serviço ou solicitação de informação. Medir a satisfação dos usuários finais com a qualidade da central de serviço e os serviços de TI.
> - **DS8.2 Registro dos Chamados dos Clientes:** Estabelecer uma função e um sistema que permitam o registro e o rastreamento de ligações, incidentes, solicitações de serviços e necessidade de informações. Deve trabalhar de perto com os processos de gerenciamento de incidentes, problemas, mudanças, capacidade e disponibilidade. Os incidentes devem ser classificados de acordo com as prioridades de negócio e serviço e direcionados à equipe adequada de gerenciamento de problemas. Os clientes devem ser mantidos informados sobre o status de seus chamados.
> - **DS8.3 Escalonamento de Incidentes:** Estabelecer os procedimentos da central de serviço para que os incidentes que não podem ser resolvidos imediatamente sejam adequadamente encaminhados, conforme os limites definidos no SLA, e soluções temporárias sejam implementadas, se aplicável. Assegurar que a propriedade e o monitoramento do ciclo de vida do incidente permaneçam com a central de serviço, independentemente do grupo de TI que esteja trabalhando nas atividades de resolução.
> - **DS8.4 Encerramento de Incidente:** Estabelecer procedimentos para o monitoramento periódico do encerramento de chamados de clientes. Quando o incidente foi resolvido, assegurar que a central de serviço registre os passos adotados para sua resolução e confirmar se as ações adotadas foram aceitas pelo cliente. Também registrar e relatar incidentes não solucionados (erros já conhecidos e alternativas existentes) para prover informações visando o adequado gerenciamento de problemas.
> - **DS8.5 Relatórios e Análises de Tendências:** Gerar relatórios de atividades da central de serviço, permitindo aos gestores medir o desempenho e o tempo de resposta dos serviços e identificar tendências ou problemas recorrentes, para que o serviço possa ser melhorado sempre

2.3.1.6 Modelo de Maturidade

Com base nos dados obtidos nos processos acima, deve ser feito a análise para calcular a maturidade da empresa, com isso consegue se valores entre 0 a 5, onde estes indicam a maturidade do negócio, que segundo o IT Governance Institute (2007) é avaliado da seguinte forma:

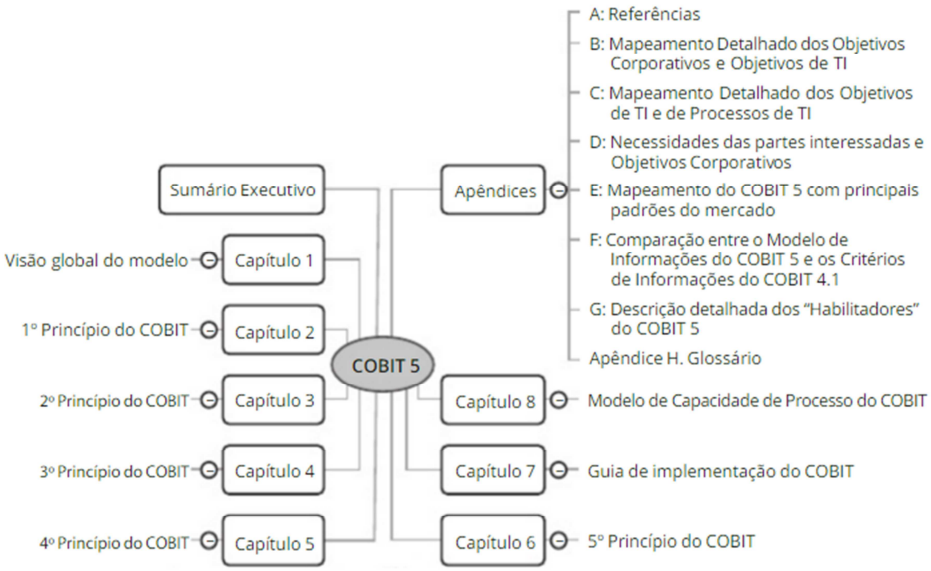
> 0. Inexistente – Completa falta de um processo reconhecido. A empresa nem mesmo reconheceu que existe uma questão a ser trabalhada.
> 1. Inicial / *Ad hoc* – Existem evidências que a empresa reconheceu que existem questões e que precisam ser trabalhadas. No entanto, não existe processo padronizado; ao contrário, existem enfoques *Ad Hoc* que tendem a ser aplicados individualmente ou caso-a-caso. O enfoque geral de gerenciamento é desorganizado.
> 2. Repetível, porém intuitivo – Os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa. Não existe um treinamento formal ou uma comunicação dos procedimentos padronizados e a responsabilidade é deixado com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e consequentemente erros podem ocorrer.
> 3. Processo Definido – Procedimentos foram padronizados, documentados e comunicados através de treinamento. É mandatório que esses processos sejam seguidos; no entanto, possivelmente desvios não serão detectados. Os procedimentos não são sofisticados, mas existe a formalização das práticas existentes.
> 4. Gerenciado e Mensurável – A gerencia monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando muito bem. Os processos estão debaixo de um constante aprimoramento e fornecem boas práticas. Automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada.
> 5. Otimizado – Os processos foram refinados a um nível de boas práticas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade como outras organizações. TI é utilizada como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e efetividade, tornando a organização rápida em adaptar-se.

2.3.2 COBIT 5

Para este trabalho de conclusão de curso, será utilizado sua versão anterior, por ser um modelo mais maduro e completo que a sua atualização, porém, vou citar sua atualização para fins acadêmicos.

O COBIT 5, segundo Reis (2015), possui um modelo para a governança corporativa de TI desenvolvido a partir de cinco princípios e baseado em sete habilitadores. Foi criado em 2013, fornecendo guias e orientações para implementação da governança de TI, que para sua publicação foi estruturado em 10 capítulos como mostra a figura a seguir:

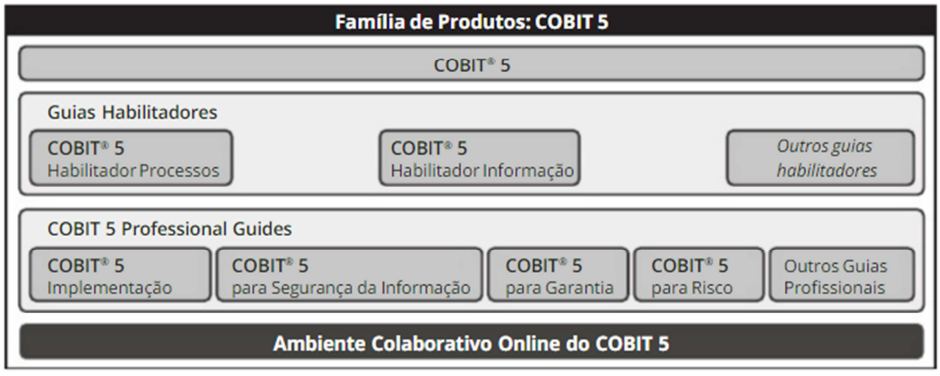
Figura 2: Estrutura para publicação do COBIT 5



Fonte: Reis (2015).

O COBIT 5 é um conjunto de publicações que foram denominados como "Família de Produtos COBIT 5":

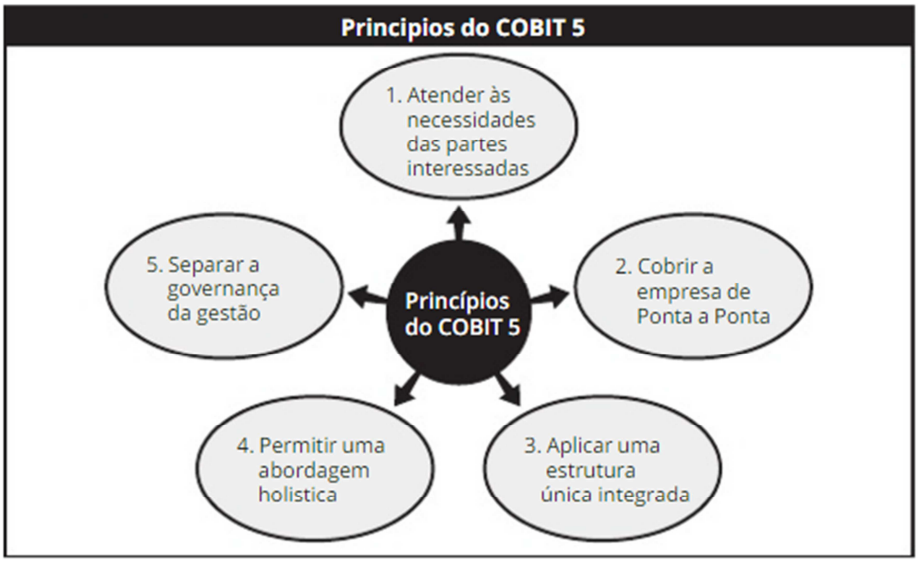
Figura 3: Família COBIT 5



Fonte: Reis (2015).

O COBIT 5 é estruturado em cinco princípios:

Figura 4: Cinco princípios do COBIT 5



Fonte: Reis (2015).

Reis (2015) ainda informa sobre as sete habilidades do COBIT 5 no tópico seguinte:

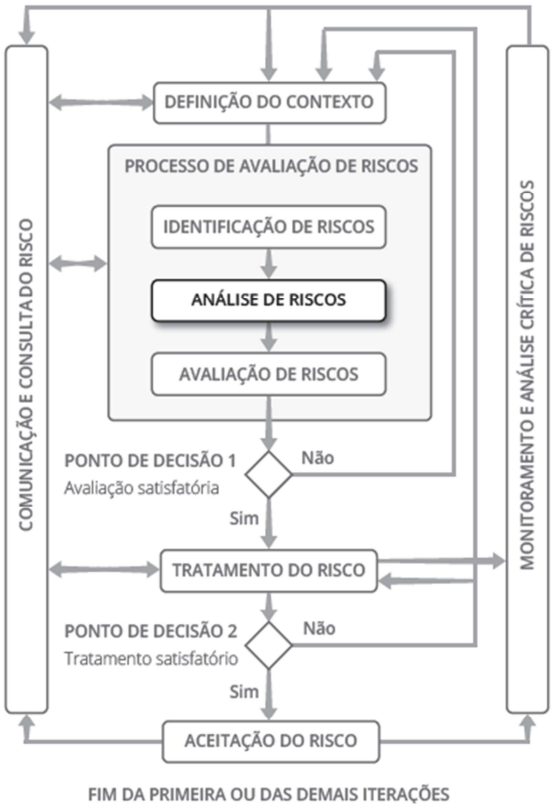
1. Princípios, Políticas e Modelos;
2. Processos;
3. Estruturas Organizacionais;
4. Cultura, Ética e Comportamento;
5. Informação;
6. Serviços, Infraestrutura e Aplicativos;
7. Pessoas, Habilidades e Competências, por meio dos quais todas as ações de governança devem ser orientadas para o alcance dos objetivos corporativos.

2.3.3 ISO/IEC 27005

De acordo com a ABNT (2002), a ISO/IEC 27001 e ISO/IEC 27002 são normas que foram preparadas com o objetivo de fornecer um modelo para melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

A ISO/IEC 27005, segundo Bezerra (2015) faz parte da série 27000, onde se incluem as normas ISO/IEC 27001 e ISO/IEC, assim, esta norma possibilita um aprofundamento nos requisitos únicos da segurança da informação, para tal, utiliza-se o diagrama de gestão de riscos para uma análise e avaliação continua dos riscos:

Figura 5: Diagrama de Gestão de Risco



Fonte: Bezerra (2015).

Pela imagem é possível verificar que para fazer a análise dos riscos é necessário seguir processos sequenciais de melhoria contínua, desta forma, Bezerra (2015) apresenta e descreve seis grandes grupos de atividades:

- Definição do contexto: responsável pela definição do ambiente, escopo, critérios de avaliação. Essencial para conhecer as informações sobre a organização.
- Análise/Avaliação de riscos: permitirá a identificação dos riscos e a determinação das ações necessárias para reduzir o risco a um nível aceitável.
- Tratamento do risco: com os resultados obtidos na análise e avaliação dos riscos são definidos os controles necessários para o tratamento dos riscos.
- Aceitação dos riscos: assegura os riscos aceitos pela organização, sendo assim, os riscos que por algum motivo não serão tratados ou serão tratados parcialmente, conhecidos como riscos residuais nas quais deverão ser justificados.
- Comunicação do risco: neste ponto é feito a comunicação dos riscos e como este será tratado para todas as áreas operacionais e seus gestores.
- Monitoramento e análise crítica: atividades de acompanhamento dos resultados, implementação dos controles e de análise para a melhoria contínua dos processos de gestão de riscos.

2.4 RESPOSTA A INCIDENTES

Já a resposta a incidentes será responsável por trazer os procedimentos do que deve ser feito caso alguma vulnerabilidade torne-se real.

Para poder entender o que é a resposta a incidentes, deve-se entender o que é um incidente. Incidente nada mais é do que uma ação ilegal, não aceitável, ou inadmissível que envolva um sistema ou rede computacional.

Esses incidentes podem ser de uso ilegal de ambientes e programas pirateados no ambiente corporativo, furto de informação ou indisponibilidade da rede.

O CERT[7] (2008) define resposta a incidentes de segurança como, "uma metodologia organizada para gerir consequências de uma violação de segurança de informação".

A resposta a incidentes está intrinsicamente ligada à missão e objetivos da empresa, pois é nela que pode-se evitar que a imagem da empresa seja danificada por eventuais incidentes, ou que seja prejudicada financeiramente, operacionalmente e até mesmo a privacidade de seus clientes.

Para que isso seja implementado deve-se criar uma equipe que suporte em todas as etapas. Na equipe é necessário que haja pessoas da área de recursos humanos, assessoria jurídica, técnica, especialistas em segurança, agentes tomadores de decisão, pessoal para a comunicação social.

Após a contratação do pessoal que atuará nos incidentes, é necessário criar um meio de treinamento contínuo e análise dos incidentes, para que tudo fique atualizado, confirmando ou descontinuando um incidente que estava registrado no procedimento.

Com a análise contínua de incidentes pode-se verificar o que realmente impacta a organização, deixando assim documentando os incidentes em um procedimento oficial. Para que um procedimento se torne oficial é necessário que haja previamente uma fase de análise e de testes dos incidentes, para confirmar se o que foi proposto em teoria acontece na operação das atividades.

[7] Centro de Estudos, Tratamentos e Respostas a Incidentes de Segurança

O conjunto das áreas Engenharia de Segurança e Engenharia de processos resulta na diminuição dos riscos e também da redução do impacto sofrido minimizando prejuízo e se recuperando do problema em pouco tempo, deixando todos preparados e avisados sobre o ocorrido.

Essas táticas também previnem a empresa de sofrer possíveis fraudes e evitar que ela pratique meios ilegais de conseguir recursos, pois para que essas duas áreas continuem em atuação e andem em conjunto com a lei é preciso que seja aplicado auditorias frequentes para averiguar se tudo está funcionando de acordo.

Essas duas áreas funcionam como meio contínuo de melhoria, pois eliminam com o tempo, problemas simples que tomam muito tempo, criando soluções para estas e deixando um tempo maior para problemas de maior complexidade, alinhando mais recursos para resolvê-los.

2.4.1 Plano de Resposta a Incidentes

De acordo com Pimenta (2008) os planos de incidentes de respostas podem ser estabelecidos por quatro palavras chaves, são elas:

- Detecção: Reportado ou Identificado;
- Triagem: Avaliar, categorizar e priorizar;
- Análise: Entender o incidente;
- Resposta: Ações para resolver o incidente;

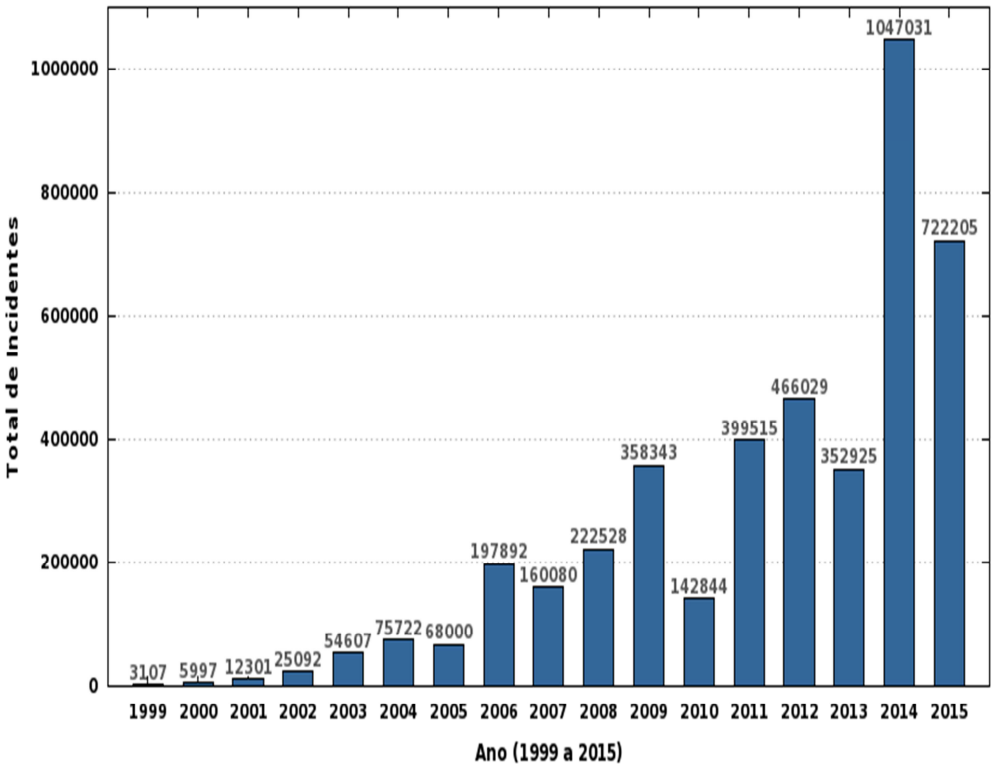
2.4.2 Tipos de Incidentes

Os incidentes de segurança são reportados ao CERT (2016), e o número aumentou drasticamente nos últimos anos.

Em 2014 os números chegaram em 1.047.031 (um milhão, quarenta e sete mil e trinta e um) incidentes reportados, mas em 2015 esse número caiu em um pouco mais de um terço.

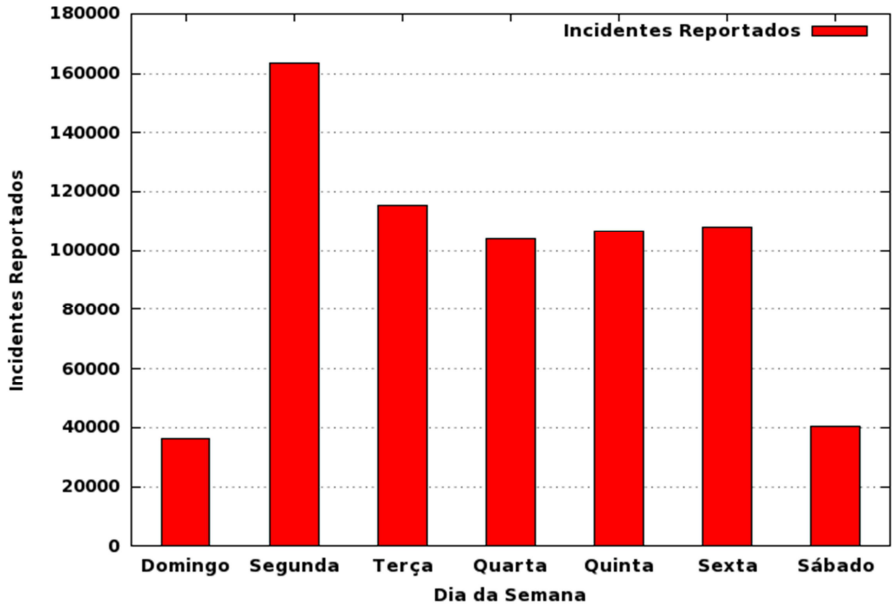
Além disso, em 2015 a segunda-feira foi o dia e que mais se reportaram ao CERT.

Figura 6: Total de Incidentes Repostados por ano



Fonte: CERT (2015).

Figura 7: Incidentes reportados por dia da semana



Fonte: CERT (2015).

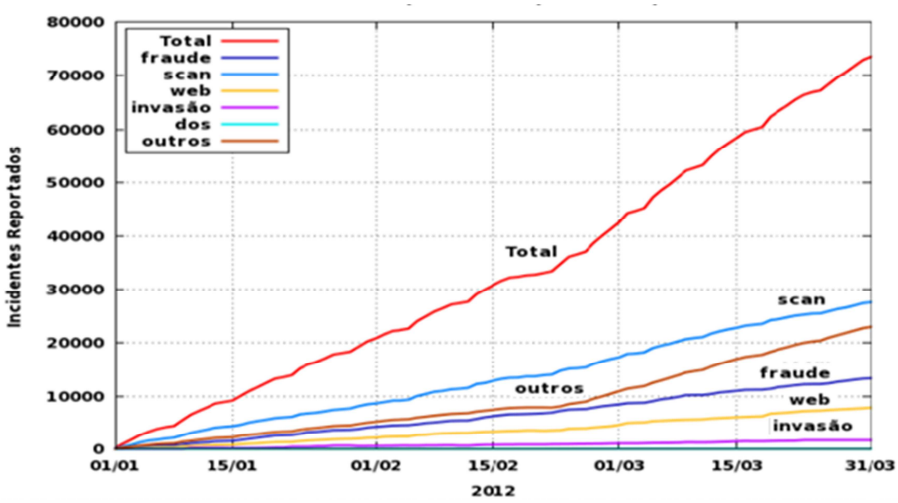
Os incidentes de segurança que são mais frequentemente reportados ao CERT (2016), são:

- Fraude de antecipação de recursos: é quando o golpista tenta induzir o usuário a fornecer as informações pessoais, ou realizar um pagamento prometendo algum tipo de benefício;
- *Scan*[8]: é a varredura de redes, em que o atacante procura por *softwares*[9] instalados para testar possível falhas de segurança ou vulnerabilidade dos mesmos;
- *Spoofing*[10]: altera o campo do e-mail do destinatário para que se parece com um e-mail enviado por outra pessoa, ou seja, falsifica a origem do e-mail;
- *Sniffing*[11]: é uma técnica que inspeciona os dados que trafegam em uma rede;

[8] Varredura de redes
[9] Programas, aplicativos ou sistemas.
[10] Falsificação de e-mail.
[11] Interceptação de tráfego

- *Brute Force*[12]: consiste em adivinhar por tentativa e erro dados de usuário e senha, para tentar acessar sites e ter acessos privilegiados no computador;
- *DDOS*[13] *(Denial of Service)*: é a técnica utilizada para tirar um serviço do ar realizada por um conjunto de computadores;
- *Malware*[14]: são programas desenvolvidos com a finalidade de realizar atividades maliciosas em um hospedeiro;
- *Spam*[15]: e-mails enviados a um grande número de usuários que possuem mensagens atrativas com o intuito de propagar golpes, códigos maliciosos e venda ilegal de produtos e serviços.

Figura 8: Tipos de ataques reportados



Fonte: CERT, (2015)

2.4.3 CSIRT

Para criar um CSIRT[16] (*Developing a Computer Security Incident Response Team*), de acordo com o CERT (2016) é necessário realizar oito passos.

[12] Força Bruta
[13] Negação de Serviço
[14] Códigos Maliciosos
[15] E-mail não solicitados
[16] Equipe de respostas a incidentes de segurança da informação.

Passo 1: Ganhar o apoio da administração;

Passo 2: Plano de desenvolvimento estratégico;

Passo 3: Coleta de dados;

Passo 4: Visão geral do CSIRT;

Passo 5: Comunicar a visão geral;

Passo 6: Iniciar implementação;

Passo 7: Divulgar o CSIRT;

Passo 8: Mensurar o CSIRT.

Os requisitos básicos para a implementação do CSIRT é a criação de um time técnico e especializado, estratégia aprovada, apoio financeiro, apoio administrativo, plano de ação aprovado, recursos físicos de TI disponíveis.

3 ESTUDO DE CASO

A empresa em que é baseado o estudo de caso é focada na prestação de serviços, e cria soluções para melhoria e continuidade do negócio. Esta também tem como foco a venda de *softwares* e serviços de suporte para outras empresas, tornando a parte de suporte e monitoração de equipamentos e softwares para outras empresas, terceirizando o serviço de TI.

A organização possui várias áreas de TI própria com times de suporte nível 2 nas áreas de Intel, Unix, Backup, Basis, Redes e Banco de Dados por exemplo. Estes ficam alocados em diversos locais, pois possuem suportes em vários países, assim variando o nível de especialização do suporte de acordo com o tipo de contrato e necessidade do cliente.

O suporte nível 1 e Serviços de atendimento ao usuário fica em sua maioria na região metropolitana de Campinas, na Índia ou nas Filipinas, fazendo o trabalho de atendimento e monitoração dos ativos da empresa.

A área de serviços de atendimento ao usuário (central de serviços) é responsável por receber incidentes reportados por usuários, inicialmente os auxiliando para problemas mais simples. Caso recebam ligações com problemas mais complexos é acionado o time de suporte nível 1.

O time de suporte nível 1 é responsável por monitorar os ativos da empresa, também são responsáveis por trabalhar em manutenções menos complexas, como por exemplo desligamento de servidores no caso de manutenção elétrica ou verificar/atualizar os servidores da organização. O suporte é responsável por acionar times de suporte nível 2 caso algum problema esteja impactando a produção da organização.

Para a análise e desenvolvimento do estudo de caso é utilizada a metodologia do COBIT 4.1 com foco nos processos de PO9, AI6, AI7, DS5 e DS8.

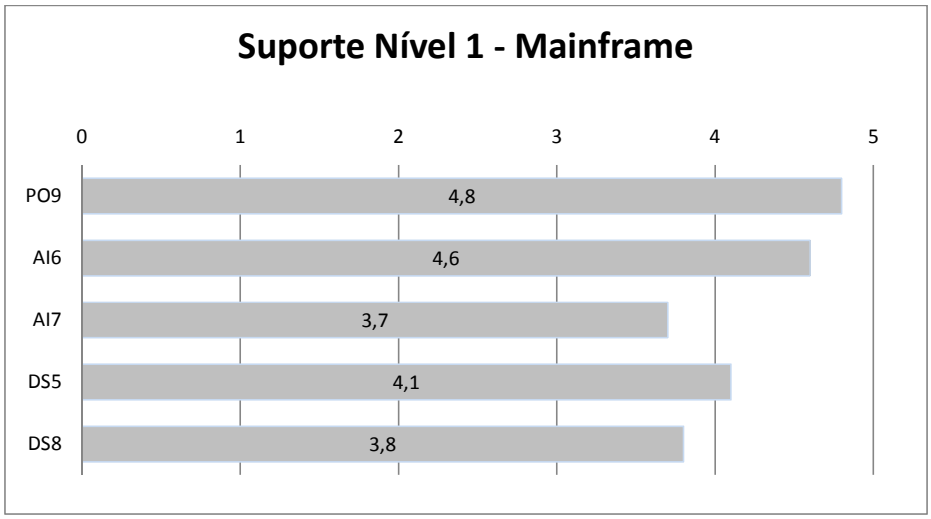
Com base nas etapas do processo descrito acima, foram realizadas perguntas para obter o cálculo e a análise da maturidade do negócio, nas quais estão anexadas a este trabalho. Estas perguntas foram respondidas por quatro times, sendo eles três de suporte nível 1 (Sistemas Distribuídos, Mainframe e Redes) e outro com o time de nível 2 (Banco de Dados). Com estes resultados é possível verificar o nível de maturidade do negócio. O questionário sendo respondido pelos líderes dos times em conjunto com os operadores dos times.

A seguir seguem os resultados da maturidade do negócio de acordo com os times entrevistados, com base nos processos mais relevantes para a análise de maturidade da organização baseados no COBIT 4.1

3.1 *MAINFRAME*

Com base no questionário, foi obtido o seguinte gráfico:

Figura 9: Suporte Nível 1 - Mainframe



Fonte: Autoria própria

Pelo gráfico é possível verificar que o time encontra-se em um nível de maturidade bem alto, visto que para os processos PO9 e AI6, encontram-se com quase nível 5, precisando de poucas sugestões de melhorias para alcançar o máximo de maturidade para o negócio.

Para o processo AI7, este encontra-se com maturidade nível 3, quase alcançando o nível 4, com certa deficiência na integração dos processos com o ciclo de vida do sistema. Possui também certa carência nos treinamentos de teste, pois pode ocorrer desvios do processo definido, possuindo bases de produção inconsistentes com os novos sistemas, podendo gerar um nível considerável de problemas após a implementação.

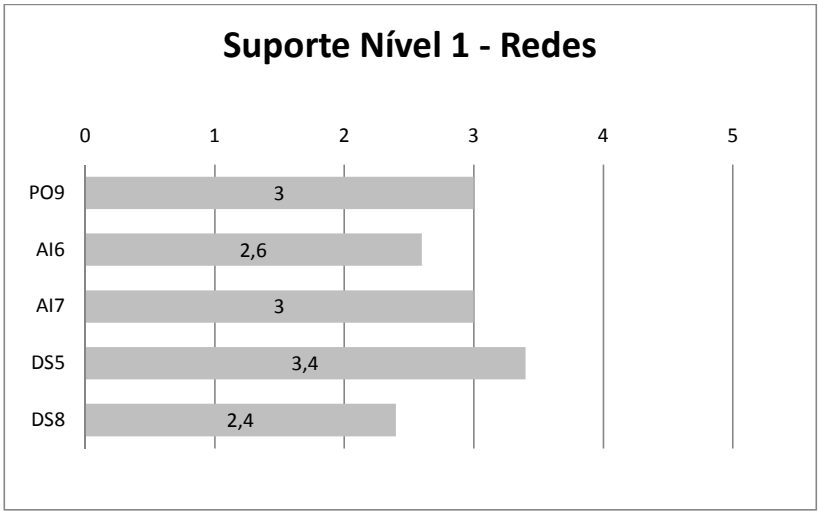
Para o processo DS5, este time possui maturidade nível 4, possuindo algumas deficiências na mensuração das métricas e objetivos de gestão de segurança, apesar deles já estarem definidos. As avaliações críticas dos riscos e impactos são executados consistentemente, porém ainda não são claramente definidos. A submissão dos métodos de segurança e a conscientização de segurança são mandatórias, mas ainda não há a responsabilidade das definições dos requisitos de segurança por parte dos usuários e clientes. Os relatórios não são feitos sistematicamente, mas estão alinhados com os objetivos de negócio.

Já para o processo DS8, o time encontra com nível de maturidade 3, quase alcançando o nível de maturidade 4. Neste caso possui uma central de serviços, porém está ainda não é bem definida ou treinada, os treinamentos ainda são de certa forma informais, os incidentes e chamados são rastreados e monitorados, porém não existe um sistema de reporte formal ou maduro, mas os usuários foram claramente comunicados sobre como registrar os problemas e incidentes.

3.2 REDES

O time de redes com base nos nas questões obteve o seguinte resultado:

Figura 10: Suporte Nível 1 - Redes



Fonte: Autoria própria

O suporte de Redes tem um nível de maturidade mediano, não conseguindo atingir nível de maturidade 4 em nenhum dos processos analisados, tendo uma média de nível 3 nos processos PO9, AI7 e DS5, nos outros processos atingindo níveis 2.

No processo PO9, o time possui processos definidos e documentados, mas não formalizados. Possui treinamento para o pessoal, mas também sendo informal, e certas decisões são deixadas para que cada um possa decidir. O time consegue identificar os riscos para os clientes, mas não de forma detalhada, a mitigação dos riscos é feita apenas após identificação dos mesmos e as responsabilidades são definidas nas descrições dos cargos.

O processo AI6, com maturidade 2, tem deficiência nos processos de gerenciamento de mudanças, sendo informais. Os processos ainda não são bem estruturados e propensos a erros. A documentação ainda é inconsistente e durante o planejamento são realizadas apenas avaliações limitadas sobre o impacto.

O processo AI7, com nível de maturidade 3, possui uma metodologia formal para alguns processos. Os processos de instalação e verificação estão interligados com o ciclo de vida do sistema, porem até certo ponto. Os treinamentos de testes ainda estão sujeitos a desvios do processo, pois ainda tem base em decisões individuais. A qualidade dos sistemas que entram em produção é inconsistente e os novos sistemas, e frequentemente geram um nível considerável de problemas após implementação.

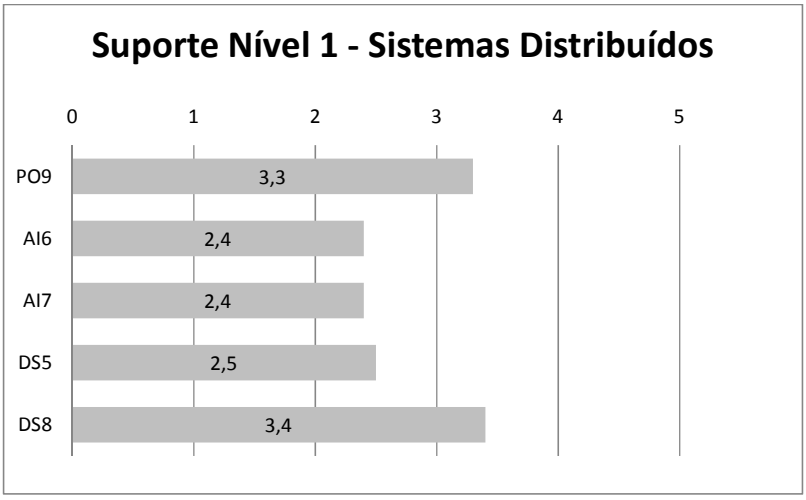
O processo DS5, está com nível de maturidade 3, a conscientização de segurança existe e é promovida pela Direção, mas ainda não é claramente atribuída. Os procedimentos de segurança são definidos e alinhados com as políticas de TI. As responsabilidades de TI ainda não são consistentemente impostas. Os relatórios do negócio ainda não têm foco na organização. Os treinamentos de segurança são disponibilizados, porém não são controlados formalmente.

E finalmente para o processo DS8, o time possui nível de maturidade 2, onde este apresenta carência na central de serviços. Este existe, porém não possui treinamento especifico, a assistência está disponível, porém não formal, não tendo ferramentas adequadas para resolução de incidentes. Os treinamentos existentes não são formais, não havendo procedimentos padronizados e comunicados. As responsabilidades ficam a cargo de cada pessoa.

3.3 SISTEMAS DISTRIBUÍDOS

O time de sistemas distribuídos, após o questionário obteve o seguinte resultado:

Figura 11: Suporte Nível 1 - Sistemas Distribuídos



Fonte: Autoria própria

Assim como o time de suporte de Redes, este apresenta um nível de maturidade baixo em relação ao nível de maturidade do time de *Mainframe*, porém este apresenta níveis de maturidade mais baixo dentro de todos os times estudados, com média de maturidade 2. Os únicos processos acima desta media são os processos PO9 e DS8.

O processo PO9, possui carência em uma avaliação e gestão de riscos com procedimentos padronizados. A gestão de risco segue processo definido e documentado. Os treinamentos estão disponíveis para todos, mas as tomadas de decisões são feitas a critério de cada indivíduo. As metodologias de avaliação dos riscos são convenientes e asseguram a identificação dos riscos mais críticos do negócio. O processo para mitigar os riscos é implementado após a identificação dos riscos. E as responsabilidades são descritas no cargo.

Para o processo AI6, com maturidade 2, possui problemas em seus processos, sendo eles geralmente informais e não bem estruturados, sem precisão nos procedimentos, e quando realizadas mudanças, estas sofrem de avaliações

básicas e limitadas sobre os impactos e processos informais de gerenciamento de mudanças.

O processo AI7, com maturidade nível 2, possui problemas com a abordagem dos testes pois elas não são baseadas em nenhuma tecnologia, mas elas possuem certa consistência no teste e na verificação. Possui certo problema também, pois a maioria das decisões são tomadas pelos times de desenvolvimento e geralmente não existe teste de integração, e possui também deficiência na aprovação, onde estas são feitas por processos informais.

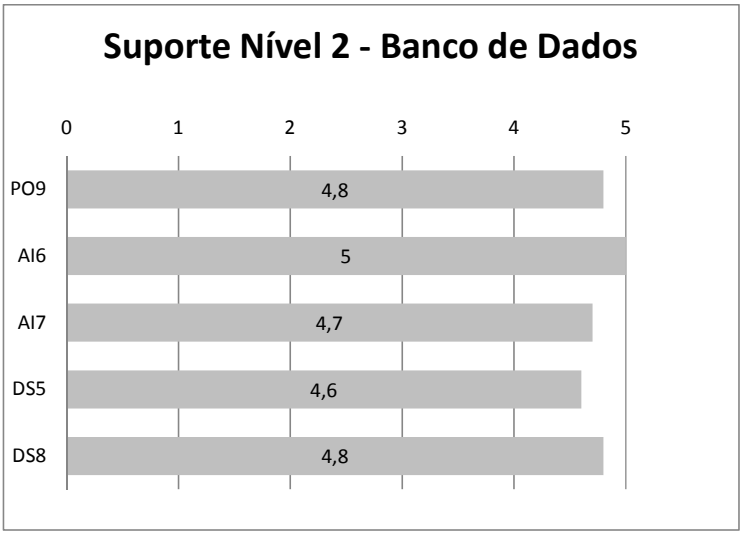
No processo DS5, com maturidade 2, possui certos problemas com as responsabilidades atribuídas para o coordenador, onde este geralmente possui autoridade limitada. Também precisam ser analisadas os problemas com as informações, onde este time produz informações relevantes, mas não são analisadas ou revisadas. Sobre as políticas de segurança, ainda estão caminhando para ser bem estruturado, mas ainda não utilizam ferramentas e habilidades adequadas. Os relatórios ainda são inconsistentes e mal elaborados. O treinamento está disponível, mas não é mandatório. A segurança de TI não é considerada como responsabilidade de todos, mas sim do time de TI.

E por fim, o processo DS8, está com nível de maturidade 3, onde já possuem uma central de serviço, porem ela não é bem estruturada nem muito bem treinada. Os procedimentos foram padronizados, mas os treinamentos ainda continuam informais, e é opcional seguir as recomendações. Neste caso, o time utiliza de sistemas de reporte, porém não são treinados adequadamente para receber os chamados e incidentes. O tempo de resposta a esses incidentes não é medido e podem continuar sem solução.

3.4 BANCO DE DADOS

Com base no questionário, foi obtido o seguinte resultado para o time de banco de dados:

Figura 12: Suporte Nível 2 - Banco de Dados



Fonte: Autoria própria

O time de banco de dados nesta pesquisa, está quase na maturidade nível 5, sendo que quase todos os processos avaliados tiveram média acima de 4,5 e um dos processos obteve maturidade nível 5, o processo AI6. Este time, para atingir nível de maturidade 5 em todos os processos, não necessita de muitas modificações e melhorias, mas necessita manter seu nível de qualidade estável.

3.5 SUGESTÕES DE MELHORIAS

Com base nas análises anteriores, foi criado sugestões de melhorias para os times de acordo com sua classificação.

***Mainframe*:** O time de *mainframe* com nível de maturidade média de 4, pode optar por seguir as seguintes sugestões de melhoria para atingir o nível de maturidade 5. Para tal, é sugerida que o time consiga obter um processo organizacional estruturado e bem gerenciado, que seja automatizado a captura, análise e relato dos dados de gestão de risco. Haja discussões para troca de experiências entre todo o time (lideres, diretores, funcionários), a gestão de risco esteja interligada as operações de negócio, é recomendado que a direção de TI consiga avaliar continuamente as estratégias de mitigação de risco.

Também é recomendado que o processo de gerenciamento de mudanças seja revisado e atualizado regularmente, para assim permanecer alinhado com as boas práticas. Os processos de revisão consigam refletir os resultados do monitoramento, que as informações de configuração sejam automatizadas por softwares que proporcionem o controle de versão. Necessita de meios mais sofisticados e ferramentas que detectam *softwares* sem licença.

Outras melhorias sugeridas são ajustes mais refinados dos processos de instalação e validação, necessitando que esses processos estejam integrados ao ciclo de vida do sistema, é sugerido que os ambientes de teste fiquem melhor desenvolvidos, registro dos problemas e processos de resolução de erros assegurados em uma migração eficiente para o ambiente de produção. É preciso que a verificação não necessite de retrabalho, bem como problemas pôs-implementação sejam padronizados.

Outras sugestões são de que os requisitos de segurança de TI estejam claramente definidos. Todos precisam entender suas responsabilidades nos requisitos de segurança. Os incidentes sejam tratados imediatamente, possuindo procedimentos formalizados apoiados em uma ferramenta automatizada. Necessário também que as avaliações de segurança sejam realizadas periodicamente, assim como testes de segurança, análise de causa-raiz.

Para finalizar, é sugerido que os processos de gerenciamento de incidentes estejam bem estabelecidos, e bem organizados, as métricas sejam sistematicamente medidas e reportadas. Que haja ferramentas que permitam aos usuários fazer diagnósticos e resolução dos incidentes. É sugerido que os incidentes sejam resolvidos rapidamente dentro de um processo de encaminhamento estruturado.

Redes: As sugestões de melhoria para o time de redes para atingir nível de maturidade 4 precisa de avaliações de gestão de riscos com procedimentos padronizados. Necessário que os riscos encontrados tenham um responsável definido e o comitê executivo possa estabelecer os níveis de riscos que podem ser tolerados. Criar indicadores para avaliar os riscos definindo taxas de riscos e retornos. Estudar estratégias para mitigar os riscos. Criar um processo de gerenciamento de mudanças bem desenvolvido, criar também processos eficazes, as mudanças sejam planejadas e avaliadas com seu impacto, minimizando as probabilidades de problemas. Criar processos formalizados para serem organizados

e práticos. Mudanças principais recebam abordagem formalizada. Avaliação de atendimento de requisitos de usuários seja padronizada e mensurável, necessita que o sistema de reses reflita o ambiente operacional.

É recomendado que as responsabilidades pela segurança de TI sejam claramente atribuídas, gerenciadas e impostas. Haja avaliações críticas dos riscos e impactos consistentemente, seja mandatória a submissão aos métodos de promoção de conscientização de segurança. A identificação, autenticação e autorização dos usuários sejam padronizados, os objetivos e métricas de gestão de segurança sejam definidos, mesmo não sendo mensurados.

Por fim, é recomendado que as ferramentas e técnicas sejam automatizadas com base no conhecimento centralizado, os profissionais da central de serviço interajam muito próximo aos profissionais de gerenciamento de problemas. As responsabilidades sejam claras e efetivamente monitoradas. O pessoal da central de serviços seja bem treinado.

Sistemas Distribuídos: As sugestões de melhoria para que o time atinja nível de maturidade 4, é necessário que este siga sugestões como, avaliações e gestão de riscos com procedimentos padronizados, o risco seja avaliado e mitigado no nível do projeto, a área de TI conseguir realocar recursos para um projeto a fim de reavaliar periodicamente os riscos, a área de TI estudar estratégias de mitigação de riscos.

Fazer com que os processos tornem-se eficazes e eficientes, as mudanças sejam sujeitas ao planejamento e avaliação de impacto para minimizar a probabilidade de problemas após a produção.

Criar processo de aprovação de mudanças, criar documentação de gerenciamento de mudanças e mantê-la atualizada. Criar procedimentos formais e estes sejam práticos e organizados. Possuir ambiente de restes e procedimentos de validação definidos.

Fazer com que os sistemas de teste reflitam o ambiente operacional. Responsabilidades pela segurança de TI sejam claramente atribuídas, avaliações críticas de risco sejam executadas consistentemente, tornar mandatório a submissão aos métodos de promoção de conscientização de segurança. Fazer com que os testes de segurança sejam realizados utilizando padrões e processos formalizados, deixar os relatórios de segurança alinhados com os objetivos de negócio.

Tornar as ferramentas e técnicas automatizadas com base de conhecimento centralizado, fazer com que os profissionais da central de serviço interajam com profissionais de gerenciamento de problemas, fazer com que o pessoal da central de serviços seja treinado e processos melhorados através do uso de *software* especifico.

Banco de dados: Para o time de banco de dados, com maturidade media quase 5, não são necessárias muitas sugestões de melhoria, necessitado de algumas poucas dicas e tentar manter a qualidade do serviço como esta.

Para atingir o nível de maturidade 5, é necessário que este possuía um gerenciamento de risco que tenha desenvolvido ao ponto de existir um processo organizacional estruturado e em gerenciado.

As boas práticas sejam aplicadas em todo o time, a captura, análise e relato dos dados estejam altamente automatizados, a gestão de riscos integrada as operações de negócio, processos de instalação e validação sejam refinados a um nível de boas práticas.

Um ambiente de testes bem desenvolvidos, revisões pós-implementação sejam padronizadas, tornar a segurança de TI responsabilidade de todos, tornar os requisitos de segurança claramente definidos, realizar avaliações de segurança periódicas para verificar a efetividade da implementação do plano de segurança. Fazer com que as informações sobre ameaças e vulnerabilidades sejam coletadas e analisadas sistematicamente. Comunicar sobre as métricas de gerenciamento de segurança.

CONSIDERAÇÕES FINAIS

A partir da apresentação e análise dos dados, observa-se que, esta empresa possui uma diferença grande de maturidade entre os times. Foi verificado que um dos motivos seja nos recursos disponibilizados aos times, pois para times com informações mais sensíveis e que causam mais impacto aos seus clientes, estes não possuem limitação tanto para recursos na infraestrutura como para recursos humanos.

Outra questão importante diz respeito à central de serviços das quais precisam de atenção especial para treinamentos e procedimentos, onde todos os times estudados sofreram de alguma forma nesta etapa.

Atrelado às questões acima citadas, pode-se hipotetizar que o negócio terá uma possível padronização entre os times, ou ao menos criar níveis de qualidade com diferenças suaves entre eles.

Assim, conclui-se que com a utilização das normas estabelecidas pela ABNT e COBIT, atreladas a análise feita no negócio, abordando seus riscos, ameaças e vulnerabilidades, obtém a melhoria do serviço prestado, e continue aplicando o plano de continuidade de melhoria do COBIT, o negócio obterá documentos mais efetivos sobre os incidentes.

REFERÊNCIAS BIBLIOGRAFICAS

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR 10520**: informação e documentação: citações em documentos: apresentação. Rio de Janeiro: ABNT, 2002. 7p.

BEST MANAGEMENT PRACTICE. Disponível em < https://www3.epa.gov/npdes/pubs/owm0274.pdf >. Acesso em: 25 abr. 2016.

BEZERRA, Edson Kowask. **Gestão de Riscos de TI - NBR 27005.** Rio de Janeiro: Rede Nacional de Ensino e Pesquisa, 2013. 138 p.

CENDROWSKI, Harry; MAIR, William C**. Enterprise risk management and COSO:** a guide for directors, executives, and practitioners. Hoboken/NJ/USA: John Willey & Sons, 2009.

CERT/CC. Computer Security Incident Response**.Team FAQ**. Disponível em: < http://www.cert.org/csirts/csirt-faq.html > Acesso em: 25 abr. 2016.

ELLIS, Juanita; SPEED, Tim. **The Internet security guidebook.** USA: Academic Press. 1º ed. 2011. (ISBN: 0223747).

ISO Online Browsing Plataform. **ISO 31000:2009.** Disponível em: < https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en > Acesso em: 19 abr. 2016.

IT GOVERNANCE INSTITUTE. **Board briefing on IT governance**. 2º Edição, USA, 2003.

IT GOVERNANCE INSTITUTE. **COBIT 4.1**: modelo, objetivos de controle, diretrizes de gerenciamento, modelos de maturidade. USA, 2007.

FENACOR. Federação Nacional das Empresas de Seguros Privados e de Capitalização. **Glossário de seguros**, 2011. Disponível em: <

http://www.fenacor.com.br/InformacoesAoPublico/GlossarioDeSeguros > Acesso em: 20 de abr. de 2016.

LA ROCQUE, Eduarda (coord). **Guia de orientação para gerenciamento de riscos corporativos**. São Paulo, SP: IBGC, 2007 (Série de Cadernos de Governança Corporativa. Disponível em: < www.icts.com.br/new/arquivos/IBGC-orientacaogerriscoscorporativos.pdf > Acesso em: 22 abr. 2016.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia do trabalho científico**. São Paulo: Editora Atlas, 1992. 4a ed.

MANSUR, RICARDO. **Governança de TI**: metodologias, frameworks e melhores práticas. Rio de Janeiro: Brasport, 2007.

PIMENTA, Roberto Moutella. **Um modelo de Melhoria de Qualidade Baseado em Processos para Tratamento de Incidentes Computacionais na Administração Pública Federal**. Universidade de Brasília Instituto de Ciências Exatas. Disponível em: < http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/roberto_moutella.pdf > Acesso em: 10 jun. 2016.

REIS, Luis Claudio Diogo. **Fundamentos do COBIT 5.** Rio de Janeiro: Rede Nacional de Ensino e Pesquisa - Rnp, 2015. 102 p.

TOMIATTI, Thalita Soares. **Governança de TI.** 2012. 40 f. TCC (Graduação) - Curso de Tecnóloga em Processamento de Dados, Faculdade de Tecnologia de São Paulo – Fatec-sp, São Paulo, 2012. Disponível em: <http://www.fatecsp.br/dti/tcc/tcc00048.pdf>. Acesso em: 10 jun. 2016.

WEILL, PETER E ROSS, JEANNE W. **Governança de TI** . Editora M.Books, 2006.

WESTERMAN, George; HUNTER, Richard. **O risco de TI: convertendo ameaças aos negócios em vantagem competitiva.** 2. ed. São Paulo: Crontec, 2008. p. 204.

APÊNDICE A - QUESTIONÁRIO MAINFRAME

Processo PO9

Etapa PO9	Questões	Valor	
PO9.1	Qual o nível de alinhamento da estrutura de gestão de riscos com a gestão da organização?	5	Bem planejado, a mesma possui um procedimento maduro.
PO9.2	É utilizada algum setor, processo de negócio para a gestão de risco?	4	Sim. Porém como não sou dessa área, não conheço o mesmo.
PO9.2	Qual a importância da gestão de risco para setor?		Tem de grande importância uma vez que atuamos diretamente no ambiente do cliente.
PO9.2	As consequências do processo parado são altos?		Sim, uma vez que impacta o ambiente do cliente e a produção do mesmo.
PO9.3	Quais as possíveis ameaças ao sistema e as vulnerabilidades encontradas?	3	Não tenho acesso ás mesmas.
PO9.4	Qual a probabilidade dessa ameaça acontecer?	5	Muito próximo de zera uma vez que manutenções e double checks para evitar o mesmo são frequentes
PO9.5	O que pode ser feito para mitigar o risco?	5	Não existe o mesmo, a ação necessária já foi feita.
PO9.6	Como os processos serão monitorados?	5	É monitorado praticamente 24/7
	MÉDIA	4.5	

Processo AI6

Etapa AI6	Questões	Valor	
AI6.1	Existe procedimentos formais para a realização das mudanças?	4	Sim, os procedimentos são maduros e bem estabelecidos.
AI6.1	Existe um padrão para a realização das mudanças?		Não, pois há vários tipos de manutenções, não possuindo padrão, dependendo da necessidade do negócio.
AI6.2	Existe uma avaliação sobre os impactos da mudança?	4	Sim, pois o mesmo é realmente necessário uma vez que é diretamente no ambiente de produção dos clientes
AI6.2	Existe uma prioridade em relação as mudanças?		Depende da necessidade de negócio do cliente.
AI6.3	No caso de mudanças emergenciais, existe algum procedimento formal para a solicitação?	5	Sim, e o mesmo é baseado em SLA e SLO
AI6.3	Existe um procedimento de autorização para a realização de mudança emergencial?		Sim, existe uma estrutura de hierarquia para o mesmo.

AI6.4	Existe algum sistema de acompanhamento das mudanças?	5	Sim, acompanhamento com base nos processos ITIL
AI6.4	Existe algum meio de comunicação sobre o status das mudanças? Sobre o andamento das mudanças?		Sim, a comunicação é feita em tempo real através de tickets.
AI6.4	Existe algum meio para garantir que as mudanças foram realizadas como planejado?		Sim, através de tickets
AI6.5	Os procedimentos são revisados periodicamente?	5	Sim, mensalmente.
	MÉDIA	4,6	

Processo AI7

Etapa AI7	Questões	Valor	
AI7.1	Existe treinamento especifico para os usuários de diferentes departamentos?	5	Sim.
AI7.2	Existe um plano para realização de testes com os padrões organizacionais com especificações para os envolvidos?	5	Sim.
AI7.3	Existe um plano de implementação e retorno?	5	Existe

AI7.4	O ambiente é seguro para a realização de testes que condiz com o ambiente operacional?	3	Não, qualquer change é realizada no ambiente de produção de cliente.
AI7.5	Existe um plano para o retorno de conversão dos dados ou mesmo de migração de infraestrutura caso haja uma falha na realização do projeto?	4	Possui uma contingencia, na qual antes de realizar a migração, a contingencia está igual ao ambiente de produção.
AI7.5	Com o plano de retorno, existe uma trilha de auditoria no caso da necessidade de retornar ao estado anterior?		Sim, o mesmo se chama backout.
AI7.6	Existe um meio de assegurar o teste das mudanças de acordo com o plano de testes definido antes da realização da mudança?	3	Depende de cada cliente.
AI7.7	Durante o plano de testes, os usuários dos departamentos estão cientes sobre as mudanças?	2	Depende do cliente.
AI7.7	É possível que os usuários dos departamentos afetados testem o ambiente de teste para que verifiquem se há algum erro e possa ser corrigido antes da implementação final?		Não

AI7.8	Quando o plano vai para o ambiente de produção, existe um meio de controlar a transferência dos sistemas alteados?	3	É encontrado ambiente paralelo apenas em um setor de extrema criticidade
AI7.8	Quando necessário, é possível haver uma comparação dos sistemas antigo com o alterado com a utilização de sistema paralelo?		É encontrado ambiente paralelo apenas em um setor de extrema criticidade
AI7.9	Existe um procedimento para os gerentes das mudanças organizacionais para garantir a realização da revisão após a implementação?	3	Existe um procedimento, mas não é seguido por completo, sendo realizado apenas no health check
	MÉDIA	3,7	

Processo DS5

Etapa DS5	Questões	Valor	
DS5.1	O mais alto nível organizacional está gerenciando a segurança de TI?	5	Sim, o time é fragmentado.
DS5.1	A gestão empresarial está alinhada com os requisitos de segurança de ti do negócio?		Sim, a empresa é de TI
DS5.2	Os planos de segurança em TI estão adequados com os requisitos de negócio?	5	Sim
DS5.2	O plano de implementação está de acordo com os investimentos necessários? (pessoas, software, hardware)		Sim, completamente

DS5.3	Cada usuário (internos, externos e temporários) possui suas atividades bem definidas?	3	Sim, os processos são fragmentados
DS5.3	Os acessos dos usuários correspondem com as especificações de atividade do setor do mesmo?		Não, as vezes faltando acesso/permissão para os usuários para trabalhar em determinados sistemas.
DS5.3	Existe algum repositório central com a identificação dos usuários e seus acessos?		Não
DS5.3	Se existe algum repositório central, este é atualizado com frequência?		Não existe
DS5.4	Existe um procedimento de gestão de usuários para solicitação, emissão, suspensão, modificação, e bloqueio de contas?	4	Sim, porém burocrático
DS5.4	A organização possui um procedimento para aprovação de concessão de direitos de acesso aos sistemas?		Sim
DS5.5	Existe algum meio de testar e monitorar a segurança de TI proativamente?	4	Sim, porém esse processo fere as políticas internas.
DS5.5	Existe uma revalidação periódica para garantir o nível de segurança apropriado?		Sim
DS5.5	Existe um registro das logs adequados?		Possui
DS5.6	Ao receber um incidente, este vem definido e comunicado claramente com suas características, para que seja tratado adequadamente?	3	Depende do autor do incidente.

DS5.7	As tecnologias mais críticas da empresa possuem tecnologia de segurança eficientes?	5	Sim
DS5.7	Para essas tecnologias críticas, a documentação para elas está guardado de forma segura?		Sim
DS5.8	Existe uma gestão para tratar as chaves criptográficas?	5	Sim
DS5.8	Dentro dessa gestão possui meios específicos, procedimentos para geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, uso e arquivamento das chaves criptográficas visando proteger contra sua modificação ou revelação pública não autorizada?		Sim
DS5.9	Possui procedimentos e mudanças para assegurar detecção e correções para vulnerabilidades nos sistemas?	3	Não possui para o nosso setor apenas ambientes críticos.
DS5.9	É realizado o processo de atualização do sistema e controles de vírus regularmente?		Possui
DS5.10	A organização possui procedimento para segurança de rede?	4	Possui
DS5.10	Nesse procedimento, possui técnicas para autorizar o acesso e controlar o fluxo de informações na rede?		Não, o acesso é livre, porém existe uma política de boas praticas

DS5.11	No caso de transação de dados confidenciais, possui meios seguros para a transferência dos dados?	4	Possui
DS5.11	Por estes meios, é possível confirmar a entrega e recebimento dos dados?		Apenas a confirmação de não envio do e-mail, pois é retornado e-mail informando que foi impossível enviar a informação.
	MÉDIA	4,1	

Processo DS8

Etapa DS8	Questões	Valor	
DS8.1	Na empresa possui uma central de serviço para que o usuário possa informar por problemas em TI no setor em que trabalham?	4	Sim
DS8.1	Nesta central de serviços, possui treinamento específicos para que saibam receber os chamados usuários?		Sim
DS8.1	Na central de serviços, os operadores da área possuem procedimentos para trabalhar com esses incidentes?		Sim
DS8.2	Existe ferramentas apropriadas para a criação e registro dos incidentes?	3	Sim
DS8.2	Os funcionários sabem como classificar os incidentes, como dar prioridade a eles?		Parcialmente
DS8.2	Quando há um problema, os usuários que reportaram o problema têm atualizações sobre o status do incidente e o que estão fazendo para que o problema seja resolvido?		Sim

DS8.3	Para incidentes que podem esperar ou que só podem ser resolvidos em outros horários, existe procedimento para informar as devidas ações para se trabalhar neles?		Sim
DS8.3	Os tickets criados permanecem na fila do suporte ou na fila da central de serviço?	3	Depende do problema.
DS8.4	Existe procedimentos para monitoramento de encerramento de chamados?		Sim, baseado em SLA
DS8.4	Para o encerramento de incidentes, é possível assegurar que as ações necessárias foram tomadas?		Sim
DS8.4	Para problemas recorrentes ou não solucionado, existe um registro para prover informações para um gerenciamento de problemas mais adequado?	4	Sim
DS8.5	é gerado relatórios das atividades da central de serviço? Para permitir assim o desempenho e o tempo de resposta dos serviços		Sim
DS8.5	Sobre os relatórios, é feito analise para que haja melhoria continua nesse setor?	5	Sim
	MÉDIA	3,8	

Média

Resultados	
PO9	4,8
AI6	4,6
AI7	3,7
DS5	4,1
DS8	3,8
Media	4,2

APÊNDICE B - QUESTIONÁRIO REDES

Processo PO9

Etapa PO9	Questões	Valor	
PO9.1	Qual o nível de alinhamento da estrutura de gestão de riscos com a gestão da organização?	3	Ainda falta muito acompanhamento do operador com o time de gerencial, acaba que por aprender no dia a dia, não havendo uma aproximação tão próxima.
PO9.2	É utilizada algum setor, processo de negócio para a gestão de risco?	4	Possui um responsável para esta área, que acaba envolvido com toda a equipe, sendo um único responsável focado para isso
PO9.2	Qual a importância da gestão de risco para setor?		Evitar que se prejudique o negócio do cliente, não impactando o cliente.
PO9.2	As consequências do processo parado são alto?		Para a nossa área, ficaria sem suporte, pois ficaria sem monitoração, ficariam desprovido de informações do negócio, principalmente de redes
PO9.3	Quais as possíveis ameaças ao sistema e as vulnerabilidades encontradas?	3	Uma queda de energia, mal funcionamento do equipamento, problemas de rede, temperatura, interface, dispositivo rodando no backup, - vulnerabilidade - datacenter, vpn, setores mais privilegiados, de produção

PO9.4	Qual a probabilidade dessa ameaça acontecer?	2	É comum de acontecer, pois envolve questões climáticas, questões de equipamentos, questão de pessoas usando a mesma rede na empresa.
PO9.5	O que pode ser feito para mitigar o risco?	2	No sistema que trabalhamos hoje, não existe uma manutenção preventiva, apenas proativa, agindo apenas quando o problema já está acontecendo
PO9.6	Como os processos serão monitorados?	4	Utiliza ferramenta própria de monitoramento, recebendo alertas divididos em 3 classes, com escalas de criticidade, com severidades baixas medias e altas.
	MÉDIA	3,0	

Processo AI6

Etapa AI6	Questões	Valor	
AI6.1	Existe procedimentos formais para a realização das mudanças?	3	Existe, possui primeiramente um e-mail com aprovação da liderança, depois de aprovado, é verificado qual o melhor horário para que esta ocorra, e escala o time de operações para cobrir os horários das manutenções
AI6.1	Existe um padrão para a realização das mudanças?		Não, pois há vários tipos de manutenções, não possuindo padrão, dependendo da necessidade do negócio.

AI6.2	Existe uma avaliação sobre os impactos da mudança?	4	Possui uma avaliação anterior do impacto da mudança
AI6.2	Existe uma prioridade em relação as mudanças?		Existe uma prioridade em relação as mudanças.
AI6.3	No caso de mudanças emergenciais, existe algum procedimento formal para a solicitação?	2	Apenas é enviado um e-mail para a realização da manutenção, com o horário que vai acontecer e com quais equipamentos serão afetados.
AI6.3	Existe um procedimento de autorização para a realização de mudança emergencial?		Não há um procedimento formal para a aprovação da change emergencial.
AI6.4	Existe algum sistema de acompanhamento das mudanças?	3	Possui, mas não possuímos acesso. Só recebemos o informativo para a realização.
AI6.4	Existe algum meio de comunicação sobre o status das mudanças? Sobre o andamento das mudanças?		E-mail ou conferencia, que acontece no momento da manutenção.
AI6.4	Existe algum meio para garantir que as mudanças foram realizadas como planejado?		Existe uma documentação para validação do sistema. Health check
AI6.5	Os procedimentos são revisados periodicamente?	1	Não existe procedimento de change.
	MÉDIA	2,6	

Processo AI7

Etapa AI7	Questões	Valor	
AI7.1	Existe treinamento especifico para os usuários de diferentes departamentos?	5	Existe treinamento especifico
AI7.2	Existe um plano para realização de testes com os padrões organizacionais com especificações para os envolvidos?	2	Não
AI7.3	Existe um plano de implementação e retorno?	4	Existe
AI7.4	O ambiente é seguro para a realização de testes que condiz com o ambiente operacional?	3	Possui um ambiente de testes, mas variando muito do setor, em setores de produção possui, mas para ambientes menos críticos, não há
AI7.5	Existe um plano para o retorno de conversão dos dados ou mesmo de migração de infraestrutura caso haja uma falha na realização do projeto?	3	Possui uma contingencia, na qual antes de realizar a migração, a contingencia está igual ao ambiente de produção.
AI7.5	Com o plano de retorno, existe uma trilha de auditoria no caso da necessidade de retornar ao estado anterior?		Existe um registro, porém não é uma documentação formal. É apenas um registro.

AI7.6	Existe um meio de assegurar o teste das mudanças de acordo com o plano de testes definido antes da realização da mudança?	3	Depende muito do setor, para setores de produção é realizado testes e estes entram de acordo com os testes de mudança, em sua grande maioria, porem em ambientes menos críticos para a empresa, as mudanças geralmente acontecem com erros, necessitando retornar para o estado inicial
AI7.7	Durante o plano de testes, os usuários dos departamentos estão cientes sobre as mudanças?	1	Não
AI7.7	É possível que os usuários dos departamentos afetados testem o ambiente de teste para que verifiquem se há algum erro e possa ser corrigido antes da implementação final?		Não
AI7.8	Quando o plano vai para o ambiente de produção, existe um meio de controlar a transferência dos sistemas alteados?	3	É encontrado ambiente paralelo apenas em um setor de extrema criticidade
AI7.8	Quando necessário, é possível haver uma comparação dos sistemas antigo com o alterado com a utilização de sistema paralelo?		É encontrado ambiente paralelo apenas em um setor de extrema criticidade
AI7.9	Existe um procedimento para os gerentes das mudanças organizacionais para garantir a realização da revisão após a implementação?	3	Existe um procedimento, mas não é seguido por completo, sendo realizado apenas no health check
	MÉDIA	3,0	

Processo DS5

Etapa DS5	Questões	Valor	
DS5.1	O mais alto nível organizacional está gerenciando a segurança de TI?	4	Existe um especifico para gerenciamento da segurança de TI.
DS5.1	A gestão empresarial está alinhada com os requisitos de segurança de ti do negócio?		De certa forma sim, pois é passado documentação da liderança para poder operar.
DS5.2	Os planos de segurança em TI estão adequados com os requisitos de negócio?	3	Sim
DS5.2	O plano de implementação está de acordo com os investimentos necessários? (pessoas, software, hardware)		Falta certo investimento, principalmente para quem trabalha com monitoração, com equipamentos mais novos.
DS5.3	Cada usuário (internos, externos e temporários) possui suas atividades bem definidas?	2	Não, pois acabam trabalhando com sistemas e áreas diferentes das definidas inicialmente
DS5.3	Os acessos dos usuários correspondem com as especificações de atividade do setor do mesmo?		Não, as vezes faltando acesso/permissão para os usuários para trabalhar em determinados sistemas.
DS5.3	Existe algum repositório central com a identificação dos usuários e seus acessos?		Existe de forma ineficiente
DS5.3	Se existe algum repositório central, este é atualizado com frequência?		Não é muito utilizado

DS5.4	Existe um procedimento de gestão de usuários para solicitação, emissão, suspensão, modificação, e bloqueio de contas?	4	Para solicitação possui documentação formal com certa burocracia
DS5.4	A organização possui um procedimento para aprovação de concessão de direitos de acesso aos sistemas?		Sim
DS5.5	Existe algum meio de testar e monitorar a segurança de TI proativamente?	2	Não, pois geralmente é trabalhado de forma reativa
DS5.5	Existe uma revalidação periódica para garantir o nível de segurança apropriado?		Não
DS5.5	Existe um registro das logs adequados?		Possui
DS5.6	Ao receber um incidente, este vem definido e comunicado claramente com suas características, para que seja tratado adequadamente?	4	Sim, geralmente em sua maioria
DS5.7	As tecnologias mais críticas da empresa possuem tecnologia de segurança eficientes?	3	Apesar de utilizar token para trabalhar, não é utilizado antivírus atualizado
DS5.7	Para essas tecnologias críticas, a documentação para elas está guardado de forma segura?		Sim

DS5.8	Existe uma gestão para tratar as chaves criptográficas?	5	Sim
DS5.8	Dentro dessa gestão possui meios específicos, procedimentos para geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, uso e arquivamento das chaves criptográficas visando proteger contra sua modificação ou revelação pública não autorizada?		Sim
DS5.9	Possui procedimentos e mudanças para assegurar detecção e correções para vulnerabilidades nos sistemas?	3	Não possui para o nosso setor apenas ambientes críticos.
DS5.9	É realizado o processo de atualização do sistema e controles de vírus regularmente?		Possui apenas para atualização de sistemas, mas não para anti- vírus
DS5.10	A organização possui procedimento para segurança de rede?	3	Possui
DS5.10	Nesse procedimento, possui técnicas para autorizar o acesso e controlar o fluxo de informações na rede?		Para fluxo de informação não. Pois é possível logar. em sites externos que podem comprometer a informação.

DS5.11	No caso de transação de dados confidenciais, possui meios seguros para a transferência dos dados?	4	Possui
DS5.11	Por estes meios, é possível confirmar a entrega e recebimento dos dados?		Apenas a confirmação de não envio do e-mail, pois é retornado e-mail informando que foi impossível enviar a informação.
	MÉDIA	3,4	

Processo DS8

Etapa DS8	Questões	Valor	
DS8.1	Na empresa possui uma central de serviço para que o usuário possa informar por problemas em TI no setor em que trabalham?	2	Sim
DS8.1	Nesta central de serviços, possui treinamento específicos para que saibam receber os chamados usuários?		Não
DS8.1	Na central de serviços, os operadores da área possuem procedimentos para trabalhar com esses incidentes?		Tem, mas não é eficiente em alguns casos
DS8.2	Existe ferramentas apropriadas para a criação e registro dos incidentes?	3	Sim
DS8.2	Os funcionários sabem como classificar os incidentes, como dar prioridade a eles?		Não
DS8.2	Quando há um problema, os usuários que reportaram o problema têm atualizações sobre o status do incidente e o que estão fazendo para que o problema seja resolvido?		Sim

DS8.3	Para incidentes que podem esperar ou que só podem ser resolvidos em outros horários, existe procedimento para informar as devidas ações para se trabalhar neles?		Sim
DS8.3	Os tickets criados permanecem na fila do suporte ou na fila da central de serviço?	3	Suporte
DS8.4	Existe procedimentos para monitoramento de encerramento de chamados?		Existe, mas não é eficiente
DS8.4	Para o encerramento de incidentes, é possível assegurar que as ações necessárias foram tomadas?		Sim, ligando para o usuário e para os times envolvidos confirmando a resolução do problema
DS8.4	Para problemas recorrentes ou não solucionado, existe um registro para prover informações para um gerenciamento de problemas mais adequado?	3	Existe um registro, porém não é formal, e é tomado muito tempo para poder ser resolvido o problema recorrente
DS8.5	é gerado relatórios das atividades da central de serviço? Para permitir assim o desempenho e o tempo de resposta dos serviços		Não existe mais, existia um cargo especifico para isso, mas que fora extinto
DS8.5	Sobre os relatórios, é feito analise para que haja melhoria continua nesse setor?	1	Não é feito mais esta análise de melhoria desde que o cargo foi extinto
	MÉDIA	2,4	

Média

Resultados	
PO9	3
AI6	2,6
AI7	3
DS5	3,4
DS8	2,4
Média	2,88

APÊNDICE C - QUESTIONÁRIO SISTEMAS DISTRIBUÍDOS

Processo PO9

Etapa PO9	Questões	Valor	
PO9.1	Qual o nível de alinhamento da estrutura de gestão de riscos com a gestão da organização?	3	No time, para certas contas, a gestão está razoável, trabalhando para conseguir estabilizar os incidentes do cliente, fazendo melhorias continuas, porém, há contas que o nível de gestão não é eficiente, fazendo com que o alinhamento seja ineficaz. Além de ser ineficaz, eles não têm pulso firme para impor decisões com o cliente, liberando ações que muitas vezes não é necessário, mas aceitando apenas pois o cliente desejou
PO9.2	É utilizada algum setor, processo de negócio para a gestão de risco?	4	Existe um processo, não muito bem definido, porem há um responsável para trabalhar nisso.
PO9.2	Qual a importância da gestão de risco para setor?		Importância alta
PO9.2	As consequências do processo parado são alto?		Para algumas contas, os processos parados causariam enorme impacto, necessitando de várias reuniões para tentar solucionar o problema.
PO9.3	Quais as possíveis ameaças ao sistema e as vulnerabilidades encontradas?	3	Servidor indisponível, cpu alto, aplicação indisponível, queda de energia, problemas climáticos

PO9.4	Qual a probabilidade dessa ameaça acontecer?	4	Há uma variação entre as contas, no geral não é muito comum de acontecer, o que recebe mesmo são alertas falsos
PO9.5	O que pode ser feito para mitigar o risco?	3	Deveria ser alinhado com o cliente, melhoria na infraestrutura
PO9.6	Como os processos serão monitorados?	3	Ferramentas de monitoração. Pager, e-mail.
	MÉDIA	3,3	

Processo AI6

Etapa AI6	Questões	Valor	
AI6.1	Existe procedimentos formais para a realização das mudanças?	3	Depende da conta, algumas são bem estruturadas e maduras, outras não existem procedimentos formais
AI6.1	Existe um padrão para a realização das mudanças?		Depende da conta, algumas possuem manutenções agendadas para o ano todo, outras não possuem esta dinâmica
AI6.2	Existe uma avaliação sobre os impactos da mudança?	2	Existe, porem esta avaliação é ineficiente, e para algumas contas não existe essa avaliação
AI6.2	Existe uma prioridade em relação as mudanças?		Não temos certeza sobre esta relação, muito provavelmente deva existir

AI6.3	No caso de mudanças emergenciais, existe algum procedimento formal para a solicitação?	3	Existe
AI6.3	Existe um procedimento de autorização para a realização de mudança emergencial?		Não existe um procedimento formal, mas é necessário aprovação de algumas pessoas importantes para conta
AI6.4	Existe algum sistema de acompanhamento das mudanças?	2	Sim, não é muito eficiente
AI6.4	Existe algum meio de comunicação sobre o status das mudanças? Sobre o andamento das mudanças?		E-mail
AI6.4	Existe algum meio para garantir que as mudanças foram realizadas como planejado?		Não existe para a nossa área, apenas executamos.
AI6.5	Os procedimentos são revisados periodicamente?	2	Não
	MÉDIA	2,4	

Processo AI7

Etapa AI7	Questões	Valor	
AI7.1	Existe treinamento especifico para os usuários de diferentes departamentos?	3	Não em todas as contas, variando de acordo com as características dos clientes
AI7.2	Existe um plano para realização de testes com os padrões organizacionais com especificações para os envolvidos?	3	Varia de acordo com o cliente.

AI7.3	Existe um plano de implementação e retorno?	3	Existe
AI7.4	O ambiente é seguro para a realização de testes que condiz com o ambiente operacional?	3	Para nossa área não, mas para alguns clientes existe ambientes de desenvolvimento
AI7.5	Existe um plano para o retorno de conversão dos dados ou mesmo de migração de infraestrutura caso haja uma falha na realização do projeto?	4	Não temos essas informações
AI7.5	Com o plano de retorno, existe uma trilha de auditoria no caso da necessidade de retornar ao estado anterior?		Não temos essas informações
AI7.6	Existe um meio de assegurar o teste das mudanças de acordo com o plano de testes definido antes da realização da mudança?	4	Tem, com a realização nos ambientes de Desenvolvimento.
AI7.7	Durante o plano de testes, os usuários dos departamentos estão cientes sobre as mudanças?	1	Não
AI7.7	É possível que os usuários dos departamentos afetados testem o ambiente de teste para que verifiquem se há algum erro e possa ser corrigido antes da implementação final?		Não

AI7.8	Quando o plano vai para o ambiente de produção, existe um meio de controlar a transferência dos sistemas alteados?	1	Não
AI7.8	Quando necessário, é possível haver uma comparação dos sistemas antigo com o alterado com a utilização de sistema paralelo?		Não
AI7.9	Existe um procedimento para os gerentes das mudanças organizacionais para garantir a realização da revisão após a implementação?	1	Não
	MÉDIA	2,4	

Processo DS5

Etapa DS5	Questões	Valor	
DS5.1	O mais alto nível organizacional está gerenciando a segurança de TI?	2	Não
DS5.1	A gestão empresarial está alinhada com os requisitos de segurança de ti do negócio?		Sim, porém não é seguido a sua totalidade

DS5.2	Os planos de segurança em TI estão adequados com os requisitos de negócio?	2	Sim, em maior parte teórico, não sendo aplicado em sua totalidade
DS5.2	O plano de implementação está de acordo com os investimentos necessários? (pessoas, software, hardware)		Falta investimento em várias partes
DS5.3	Cada usuário (internos, externos e temporários) possui suas atividades bem definidas?	2	Sim, porém não é bem executado, nem bem definido
DS5.3	Os acessos dos usuários correspondem com as especificações de atividade do setor do mesmo?		Não, pois geralmente não temos permissão para executar alguns processos.
DS5.3	Existe algum repositório central com a identificação dos usuários e seus acessos?		Existe, mas não é utilizado
DS5.3	Se existe algum repositório central, este é atualizado com frequência?		Não

DS5.4	Existe um procedimento de gestão de usuários para solicitação, emissão, suspensão, modificação, e bloqueio de contas?	3	Existe, porém não funciona corretamente, dependendo da conta
DS5.4	A organização possui um procedimento para aprovação de concessão de direitos de acesso aos sistemas?		Sim, porem sofre alguns problemas para permissões, não sendo bem aplicado
DS5.5	Existe algum meio de testar e monitorar a segurança de TI proativamente?	2	Não possuo resposta para isso
DS5.5	Existe uma revalidação periódica para garantir o nível de segurança apropriado?		Deve existir, porem o período para tal é muito longo
DS5.5	Existe um registro das logs adequados?		Deve existir, porém não é no nosso departamento
DS5.6	Ao receber um incidente, este vem definido e comunicado claramente com suas características, para que seja tratado adequadamente?	3	Nem sempre, dependendo do sistema e do cliente, vem com o sumario de forma incompreensível. E quando vem de criação manual, está muito suscetível a erros humanos e falta de dados
DS5.7	As tecnologias mais críticas da empresa possuem tecnologia de segurança eficientes?	3	Sim
DS5.7	Para essas tecnologias críticas, a documentação para elas está guardada de forma segura?		Não

DS5.8	Existe uma gestão para tratar as chaves criptográficas?	1	Não
DS5.8	Dentro dessa gestão possui meios específicos, procedimentos para geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, uso e arquivamento das chaves criptográficas visando proteger contra sua modificação ou revelação pública não autorizada?		Não
DS5.9	Possui procedimentos e mudanças para assegurar detecção e correções para vulnerabilidades nos sistemas?	3	Sim, porém não tenho conhecimento sobre
DS5.9	É realizado o processo de atualização do sistema e controles de vírus regularmente?		Depende da conta sim
DS5.10	A organização possui procedimento para segurança de rede?	3	Sim
DS5.10	Nesse procedimento, possui técnicas para autorizar o acesso e controlar o fluxo de informações na rede?		Não

DS5.11	No caso de transação de dados confidenciais, possui meios seguros para a transferência dos dados?	4	Sim
DS5.11	Por estes meios, é possível confirmar a entrega e recebimento dos dados?		Sim, existe um meio de confirmação no e-mail, este informa o envio e o recebimento dos dados
	MÉDIA	2,5	

Processo DS8

Etapa DS8	Questões	Valor	
DS8.1	Na empresa possui uma central de serviço para que o usuário possa informar por problemas em TI no setor em que trabalham?	3	Sim
DS8.1	Nesta central de serviços, possui treinamento específicos para que saibam receber os chamados usuários?		Existe, porém não é eficiente e não muito satisfatório
DS8.1	Na central de serviços, os operadores da área possuem procedimentos para trabalhar com esses incidentes?		Tem, mas não é eficiente em alguns casos

DS8.2	Existe ferramentas apropriadas para a criação e registro dos incidentes?		Sim
DS8.2	Os funcionários sabem como classificar os incidentes, como dar prioridade a eles?		Não
DS8.2	Quando há um problema, os usuários que reportaram o problema têm atualizações sobre o status do incidente e o que estão fazendo para que o problema seja resolvido?	4	Sim
DS8.3	Para incidentes que podem esperar ou que só podem ser resolvidos em outros horários, existe procedimento para informar as devidas ações para se trabalhar neles?		Sim
DS8.3	Os tickets criados permanecem na fila do suporte ou na fila da central de serviço?	4	Depende da conta
DS8.4	Existe procedimentos para monitoramento de encerramento de chamados?		Sim, para as contas que requerem o encerramento em nosso time
DS8.4	Para o encerramento de incidentes, é possível assegurar que as ações necessárias foram tomadas?		Não
DS8.4	Para problemas recorrentes ou não solucionado, existe um registro para prover informações para um gerenciamento de problemas mais adequado?	4	Existe, no próprio ticket

DS8.5	é gerado relatórios das atividades da central de serviço? Para permitir assim o desempenho e o tempo de resposta dos serviços		Existe ferramentas para gerar relatórios, porém não é utilizado nem inserido de forma correta para geração de relatório
DS8.5	Sobre os relatórios, é feito analise para que haja melhoria continua nesse setor?	2	Existe um relatório, porém não é feito a análise para melhoria
	MÉDIA	3,4	

Média

Resultados	
PO9	3,3
AI6	2,4
AI7	2,4
DS5	2,5
DS8	3,4
Média	2,8

APENDICE D - QUESTIONÁRIO BANCO DE DADOS

Processo PO9

Etapa PO9	Questões	Valor	
PO9.1	Qual o nível de alinhamento da estrutura de gestão de riscos com a gestão da organização?	5	No meu departamento, temos uma pessoa responsável por endereçar os chamados DPP (Defect prevention) portanto considero que existe um alinhamento entre gestão e suporte. Além disso, a classificação de riscos dentro de cada um dos incidentes mantém o time de suporte sempre atento a riscos ao negócio do cliente.
PO9.2	É utilizada algum setor, processo de negócio para a gestão de risco?		Existe um responsável no departamento que endereça os riscos e melhorias internas. Além disso temos contato com outro departamento que efetua um controle de todas as exigências de segurança em contrato.
PO9.2	Qual a importância da gestão de risco para setor?		Fundamental, afinal um time que cuida de banco de dados precisa estar atento aos riscos e atuar de maneira preventiva e reativa, a fim de garantir a segurança das aplicações e seus dados.
PO9.2	As consequências do processo parado são alto?		Além de multa prevista em contrato, dependendo da criticidade da aplicação, pode impactar diretamente o negócio do cliente.

PO9.3	Quais as possíveis ameaças ao sistema e as vulnerabilidades encontradas?	4	Acesso indevido das informações do banco por falhas de segurança, falhas de discos comprometendo integridade dos dados e disponibilidade, falhas de software do SGBD, ataques explorando software desatualizados, falhas humanas comprometendo a disponibilidade dos dados.
PO9.4	Qual a probabilidade dessa ameaça acontecer?	5	Falhas de software e equipamentos não são frequentes, e nem sempre as mesmas afetam a disponibilidade do banco de dados. Tentativa de acesso indevido das informações e ataques explorando vulnerabilidades de segurança do software são muito raras, quase nulas.
PO9.5	O que pode ser feito para mitigar o risco?	5	Fazemos manutenções preventivas e corretivas para minimizar todos os riscos encontrados. Existe um controle bastante eficiente dos principais componentes de segurança. Parte do controle é feito internamente, e parte é feito por um outro departamento.
PO9.6	Como os processos serão monitorados?	5	Através de controles internos executados por um responsável, controles externos feitos por outro departamento periodicamente, auditorias e utilizando uma ferramenta de gestão de incidentes.
	MÉDIA	4,8	

Processo AI6

Etapa AI6	Questões	Valor	
AI6.1	Existe procedimentos formais para a realização das mudanças?	5	Todas as mudanças são planejadas com antecedência, registradas em uma ferramenta de gestão de mudanças, aprovadas e analisadas por todos os times envolvidos, agendadas para o horário de menor impacto e discutidas semanalmente em 2 reuniões antes que a mesma esteja pronta pra execução.
AI6.1	Existe um padrão para a realização das mudanças?		Sim, mudanças de baixo risco e impacto são executadas em qualquer horário. Já as mudanças com indisponibilidade de aplicações são executadas durante a janela de manutenção de domingo.
AI6.2	Existe uma avaliação sobre os impactos da mudança?	5	Possui uma avaliação anterior do impacto da mudança
AI6.2	Existe uma prioridade em relação as mudanças?		Existe uma prioridade em relação as mudanças.
AI6.3	No caso de mudanças emergenciais, existe algum procedimento formal para a solicitação?	5	Mudanças emergenciais precisam de um incidente severidade 1, e aprovação do SDM da conta
AI6.3	Existe um procedimento de autorização para a realização de mudança emergencial?		A mudança emergencial só é executada com a aprovação do SDM. Geralmente os times impactados são notificados previamente.

AI6.4	Existe algum sistema de acompanhamento das mudanças?	5	Existe uma ferramenta de gestão de mudanças
AI6.4	Existe algum meio de comunicação sobre o status das mudanças? Sobre o andamento das mudanças?		E-mail, conferencias, e a própria ferramenta de gestão de mudanças acompanha o status de cada uma das tarefas realizadas.
AI6.4	Existe algum meio para garantir que as mudanças foram realizadas como planejado?		As evidências são anexadas na ferramenta de gestão de mudanças e o owner de mudança fica responsável por conferir se tudo foi executado como planejado, o mesmo registra a mudança como sucesso ou falha.
AI6.5	Os procedimentos são revisados periodicamente?	5	Todos os procedimentos da conta são revisados periodicamente.
	MÉDIA	5,0	

Processo AI7

Etapa AI7	Questões	Valor	
AI7.1	Existe treinamento especifico para os usuários de diferentes departamentos?	5	Existe treinamento especifico
AI7.2	Existe um plano para realização de testes com os padrões organizacionais com especificações para os envolvidos?	5	Geralmente todas as mudanças são efetuadas em sistemas de desenvolvimento e teste, e depois aplicadas a produção.
AI7.3	Existe um plano de implementação e retorno?	5	Todas as mudanças têm um plano para retornar ao estado anterior

AI7.4	O ambiente é seguro para a realização de testes que condiz com o ambiente operacional?	5	Sim, existem ambientes com cargas muito próximas das de produção e os mesmos são atualizados com frequência para refletir a realidade de produção da maneira mais fiel possível.
AI7.5	Existe um plano para o retorno de conversão dos dados ou mesmo de migração de infraestrutura caso haja uma falha na realização do projeto?	5	Backups são realizados antes de mudanças envolvendo infra do banco de dados.
AI7.5	Com o plano de retorno, existe uma trilha de auditoria no caso da necessidade de retornar ao estado anterior?		As evidências são colocadas na ferramenta de gestão de mudança e o dono da change faz a verificação.
AI7.6	Existe um meio de assegurar o teste das mudanças de acordo com o plano de testes definido antes da realização da mudança?	4	Os times responsáveis devem seguir o plano que foi estipulado na mudança, mas não existem controles para todas as ações executadas. Geralmente só é necessário uma evidencia ao final da mudança mostrando o resultado atingido.
AI7.7	Durante o plano de testes, os usuários dos departamentos estão cientes sobre as mudanças?	5	Sim, os times envolvidos são notificados e fazem parte da aprovação da mudança.
AI7.7	É possível que os usuários dos departamentos afetados testem o ambiente de teste para que verifiquem se há algum erro e possa ser corrigido antes da implementação final?		Sim, após as mudanças em teste, as mesmas são validadas e testadas para depois serem executadas em produção.

AI7.8	Quando o plano vai para o ambiente de produção, existe um meio de controlar a transferência dos sistemas alteados?		Sim, o resultado das mudanças é registrado na ferramenta de gestão de mudanças e validada com o owner.
AI7.8	Quando necessário, é possível haver uma comparação dos sistemas antigo com o alterado com a utilização de sistema paralelo?	4	Apenas é possível verificar através do registro de mudanças quais partes do sistema foram alterados, mas os valores antigos não são registrados.
AI7.9	Existe um procedimento para os gerentes das mudanças organizacionais para garantir a realização da revisão após a implementação?	4	A revisão das mudanças é feita pelo responsável pela change, apenas.
	MÉDIA	4,7	

Processo DS5

Etapa DS5	Questões	Valor	
DS5.1	O mais alto nível organizacional está gerenciando a segurança de TI?	5	Existe um específico para gerenciamento da segurança de TI.
DS5.1	A gestão empresarial está alinhada com os requisitos de segurança de ti do negócio?		Sim, todas as informações e requisitos de segurança são repassados aos suportes. Além de um focal responsável dentro do departamento contamos também com um time de controle de segurança em outro departamento.

DS5.2	Os planos de segurança em TI estão adequados com os requisitos de negócio?	4	Sim
DS5.2	O plano de implementação está de acordo com os investimentos necessários? (pessoas, software, hardware)		Os investimentos realizados dependem do cliente, e do nível de criticidade da aplicação. O cliente em que trabalho atualmente não utiliza equipamentos e recursos de ponta para infraestrutura de banco de dados.
DS5.3	Cada usuário (internos, externos e temporários) possui suas atividades bem definidas?	5	Sim, existe escopo bem definido entre os diversos times e separação de atividades dentro do próprio time
DS5.3	Os acessos dos usuários correspondem com as especificações de atividade do setor do mesmo?		Sim, parte do acesso ao banco de dados é efetuada pelo meu time. Todos os pedidos de acessos são registrados, revisados e aprovados pelo business owner.
DS5.3	Existe algum repositório central com a identificação dos usuários e seus acessos?		Existe registro em um banco de dados.
DS5.3	Se existe algum repositório central, este é atualizado com frequência?		Atualizado frequentemente e controles periódicos são realizados.

DS5.4	Existe um procedimento de gestão de usuários para solicitação, emissão, suspensão, modificação, e bloqueio de contas?	5	Existe um processo para cada uma das ações mencionadas.
DS5.4	A organização possui um procedimento para aprovação de concessão de direitos de acesso aos sistemas?		Sim
DS5.5	Existe algum meio de testar e monitorar a segurança de TI proativamente?	5	Sim, são executados tanto internamente como por um time de outro departamento. Como exemplo health checks aos sistemas.
DS5.5	Existe uma revalidação periódica para garantir o nível de segurança apropriado?		Sim, periodicamente.
DS5.5	Existe um registro das logs adequados?		Possui
DS5.6	Ao receber um incidente, este vem definido e comunicado claramente com suas características, para que seja tratado adequadamente?	4	Sim, a maioria dos incidentes é gerado por uma ferramenta de automação e, portanto, são alertas bem definidos. Quando são abertos chamados através de helpdesks as vezes algumas informações fundamentais não são fornecidas, o que atrasa a atuação do suporte.

DS5.7	As tecnologias mais críticas da empresa possuem tecnologia de segurança eficientes?	5	Sim, além de uma rede bem protegida, acessos bem controlados, é empregado autenticação em 2 passos para algumas aplicações. Além disso controles de acesso são feitos de maneira periódica.
DS5.7	Para essas tecnologias críticas, a documentação para elas está guardada de forma segura?		Sim
DS5.8	Existe uma gestão para tratar as chaves criptográficas?	5	Sim
DS5.8	Dentro dessa gestão possui meios específicos, procedimentos para geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, uso e arquivamento das chaves criptográficas visando proteger contra sua modificação ou revelação pública não autorizada?		Sim

DS5.9	Possui procedimentos e mudanças para assegurar detecção e correções para vulnerabilidades nos sistemas?	5	Sim
DS5.9	É realizado o processo de atualização do sistema e controles de vírus regularmente?		Sim
DS5.10	A organização possui procedimento para segurança de rede?	3	Sim
DS5.10	Nesse procedimento, possui técnicas para autorizar o acesso e controlar o fluxo de informações na rede?		Para fluxo de informação não. Pois é possível logar em sites externos que podem comprometer a informação.
DS5.11	No caso de transação de dados confidenciais, possui meios seguros para a transferência dos dados?	5	Possui
DS5.11	Por estes meios, é possível confirmar a entrega e recebimento dos dados?		Sim
	MÉDIA	4,6	

Processo DS8

Etapa DS8	Questões	Valor	
DS8.1	Na empresa possui uma central de serviço para que o usuário possa informar por problemas em TI no setor em que trabalham?		Sim
DS8.1	Nesta central de serviços, possui treinamento específicos para que saibam receber os chamados usuários?		Sim
DS8.1	Na central de serviços, os operadores da área possuem procedimentos para trabalhar com esses incidentes?	5	Sim
DS8.2	Existe ferramentas apropriadas para a criação e registro dos incidentes?		Sim
DS8.2	Os funcionários sabem como classificar os incidentes, como dar prioridade a eles?		Sim
DS8.2	Quando há um problema, os usuários que reportaram o problema têm atualizações sobre o status do incidente e o que estão fazendo para que o problema seja resolvido?	5	Sim

DS8.3	Para incidentes que podem esperar ou que só podem ser resolvidos em outros horários, existe procedimento para informar as devidas ações para se trabalhar neles?		Sim
DS8.3	Os tickets criados permanecem na fila do suporte ou na fila da central de serviço?	4	Suporte
DS8.4	Existe procedimentos para monitoramento de encerramento de chamados?		A própria ferramenta tem um controle sobre encerramentos.
DS8.4	Para o encerramento de incidentes, é possível assegurar que as ações necessárias foram tomadas?		Sim, na maioria dos casos é anexada uma evidência e uma explicação sobre causa e resolução do incidente
DS8.4	Para problemas recorrentes ou não solucionado, existe um registro para prover informações para um gerenciamento de problemas mais adequado?	5	Existe um controle interno para melhorias onde são registrados os incidentes mais frequentes. A partir disso são tomadas ações para resolver de maneira permanente o problema.

DS8.5	é gerado relatórios das atividades da central de serviço? Para permitir assim o desempenho e o tempo de resposta dos serviços	5	Métricas são geradas para analisar quais as principais atividades do time.
DS8.5	Sobre os relatórios, é feito analise para que haja melhoria continua nesse setor?		Existe um responsável no departamento que realiza essa análise
	MÉDIA	4,8	

Média

Resultados	
PO9	4,8
AI6	5
AI7	4,7
DS5	4,6
DS8	4,8
Media	4,78