LUCIANO JOHNSON

PROPOSTA DE UMA ESTRUTURA DE ANÁLISE DE MATURIDADE DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO COM BASE NA NORMA ABNT NBR ISO/IEC 27002:2005

Dissertação apresentada ao Programa de Pós-Graduação em Ciência, Gestão e Tecnologia da Informação, do Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná, como parte das exigências para obtenção do título de Mestre.

Orientador: Prof. Dr. José Simão de Paula Pinto.

CURITIBA

2012

TERMO DE APROVAÇÃO

Luciano Johnson

"PROPOSTA DE UMA ESTRUTURA DE ANÁLISE DE MATURIDADE DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO COM BASE NA NORMA ABNT NBR ISO/IEC 27002:2055"

DISSERTAÇÃO APROVADA COMO REQUISITO PARCIAL PARA OBTENÇÃO DO GRAU DE MESTRE NO PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA, GESTÃO E TECNOLOGIA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO PARANÁ, PELA SEGUINTE BANCA EXAMINADORA:

Prof. Dr. José Simão de Paula Pinto
(Orientador/UFPR)

Prof. Dr. Sérgio Scheer
(Examinador/UFPR)

Prof. Dr. Edelvino Razzolini Filho
(Examinador/UFPR)

23 de fevereiro de 2012

À Jackeline, minha esposa, e a minha filha Luana.
Por todos os dias, pelo amor e pela compreensão de vocês e por estarmos juntos em mais esta conquista.

AGRADECIMENTOS

A Deus, por diariamente iluminar meu caminho, me dando força, proteção e todo seu amor.

Ao professor José Simão, pela orientação, apoio e principalmente por acreditar no meu sonho que virou realidade.

Ao professor Sergio Scheer, pelas incansáveis conversas, motivações e colaboração em todas as fases de minha formação acadêmica.

Aos professores do Programa de Pós-Graduação em Ciência, Gestão e Tecnologia da Informação, pelas lições de vida e acadêmicas, sempre estando à disposição para nossa evolução.

Aos funcionários da Coordenação do Programa de Pós-Graduação em Ciência, Gestão e Tecnologia da Informação, especialmente a você, Esther.

À IT7 Sistemas, representada por João Batista Comelli, que sempre me serviu de referência profissional e me forneceu apoio na construção de minha carreira.

À ISACA, por ter sido a fonte de inspiração deste projeto de pesquisa.

Gerenciamento é substituir músculos por pensamentos, folclore e superstição por conhecimento, e força por cooperação.

Peter Drucker

SUMÁRIO

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

ABNT	– Associação Brasileira de Normas Técnicas
AND	– Acordo de Não Divulgação
CMMI	– *Capability Maturity Model Integration*
COBIT	– *Control Objectives for Information and Related Technology*
DSIC	– Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República
IEC	– *International Electrotechnical Commission*
ITGI	– *Information Technology Governance Institute*
ITIL	– *Information Technology Infrastructure Library*
ISO	– *International Organization for Standardization*
NBR	– Denominação de norma da Associação Brasileira de Normas Técnicas
OCDE	– Organização para a Cooperação e o Desenvolvimento Econômico
PDCA	– *Plan, Do, Check, Act*
PHP	– *Hypertext Preprocessor*
PMI	– *Project Management Institute*
SEFTI	– Secretaria de Fiscalização de Tecnologia da Informação
TCU	– Tribunal de Contas da União
TI	– Tecnologia da Informação

RESUMO

Os conceitos e práticas de segurança da informação têm evoluído nos últimos anos, e as empresas têm buscado se adaptar a esta evolução. O esforço para esta adaptação reflete, na maioria das vezes, a visão da tecnologia da informação. Neste contexto é possível identificar a necessidade de um modelo para avaliar como a segurança da informação é tratada nas organizações. A segurança da informação não possui uma estrutura de processos ou mesmo um modelo de maturidade que apoie as organizações na identificação de melhorias. Este trabalho tem por objetivo propor uma estrutura de análise de maturidade dos processos de segurança da informação com base na norma ABNT NBR ISO/IEC 27002:2005 que busque fechar a lacuna identificada anteriormente. Para alcançar este objetivo foram modelados processos com base na norma de segurança da informação ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005). Os processos foram derivados dos objetivos de controle estabelecidos na norma técnica e as atividades dos processos foram derivadas dos controles de cada objetivo de controle normativo. A partir deste ponto foi utilizado o modelo genérico de maturidade, proposto pelo CMMI e amplamente utilizado em boas práticas internacionais, para se desenvolver os modelos de maturidade dos processos de segurança da informação. Para avaliar a maturidade através dos modelos propostos, foi desenvolvido um questionário de análise de maturidade e uma ferramenta computacional para apoiar a aplicação do mesmo. O questionário foi aplicado em dez organizações da região de Curitiba-PR, que possuem acima de mil usuários internos de tecnologia da informação. Os resultados indicam que o tema ainda é foco da área de tecnologia da informação - TI, pois somente os processos diretamente relacionados com a TI se mostraram mais evoluídos. Por outro lado, os processos relacionados à gestão e planejamento se mostraram os menos desenvolvidos. Através das análises foi possível concluir que a segurança da informação é abordada como uma responsabilidade de TI e não corporativa. Outra conclusão importante é que o tema é ainda novo nas organizações, pela baixa maturidade dos processos identificada na pesquisa. Isso sugere que de fato existem melhorias a serem desenvolvidas, principalmente nas questões de gestão da segurança da informação.

Palavras-chave: Segurança da informação. Maturidade de processo. Gestão de processo. CMMI.

ABSTRACT

The concepts and information security practices have evolved in recent years and companies have sought to adapt to this evolution. The effort for this adaptation reflects, in most cases, the vision of information technology. In this context it is possible to identify the need for a model to assess how information security is handled in organizations. Information security does not have a process structure or even a maturity model to support organizations in identifying improvements. This paper aims to propose a framework for analysis of information security process maturity based on standard ABNT NBT ISO/IEC 27002:2005 that seeks to close the gap identified above. To achieve this objective processes were modeled based on the information security standard ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005). The processes were derived from the control objectives set out in the technical standard and the activities of these processes were derived from the controls of each control objective normative. From this point was used the generic maturity model proposed by CMMI and widely used in international practice, to develop models of information security maturity process. In order to evaluate the maturity through the proposed models, a questionnaire was developed for the analysis of maturity and a computational tool to support the application. The questionnaire was administered in ten organizations in the region of Curitiba-PR-Brazil, which have over one thousand internal users of information technology. The results indicate that the theme is still the focus of information technology area - IT, because only the processes directly related to IT were more evolved. On the other hand, processes related to planning and management proved the least developed. Through the analysis it was concluded that information security is addressed as an IT responsibility rather than corporate responsibility. Another important conclusion is that the subject is still new in organizations, because the low processes maturity identified in the survey. This suggests that in fact there are improvements to be developed mainly on the management of information security.

Keywords: Information security. Process maturity. Process management. CMMI.

1 INTRODUÇÃO

As organizações têm buscado desenvolver diferenciais competitivos, utilizando novas tecnologias, novos conceitos e principalmente novos ambientes. Muitos partiram da computação centralizada, outros da computação distribuída e os mais visionários da computação em nuvem. Mas em todos estes ambientes, a preocupação com a segurança é a mesma, e sempre parece insuficiente. A evolução das tecnologias de informação e comunicação tem feito com que organizações enfrentem novos desafios no que diz respeito à Segurança da Informação (CANONGIA e MANDARINO JUNIOR, 2009). A velocidade com que as informações são geradas e trocadas está em constante aceleração, fazendo com que os seus proprietários não se atentem a questões mais específicas como confidencialidade, integridade e disponibilidade, os pilares da segurança da informação (ABNT, 2005).

Em seu artigo “Segurança cibernética: o desafio da nova Sociedade da Informação”, Canongia e Mandarino Junior (2009) apresentam informações sobre o nível de preocupação das organizações sobre o tema Segurança da Informação da reunião da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE, 2012) ocorrida em março de 2009. Os principais pontos a serem destacados sobre esta nova Sociedade da Informação foram: a) convergência de tecnologias, aumento significativo de sistemas e redes de informação, aumento crescente de acesso à Internet, avanços das tecnologias de informação e comunicação; b) aumento das ameaças e das vulnerabilidades, apontando para a urgência de ações na direção da criação, manutenção e fortalecimento da cultura de segurança; c) ambiente em constantes e rápidas mudanças. A OCDE surgiu na década de 1960, quando 18 países europeus mais os Estados Unidos e o Canadá juntaram forças para criar uma organização dedicada ao desenvolvimento global (OCDE, 2012). Atualmente, fazem parte da OCDE 34 países membros que abrangem todo o globo (América do Norte, América do Sul, Europa e região da Ásia-Pacífico). Este grupo inclui muitos dos países mais avançados do mundo, mas também países emergentes como México, Chile e Turquia. Assim como conta com a estreita colaboração com os gigantes emergentes como China, Índia e Brasil e as economias em desenvolvimento na África, Ásia, América Latina e do Caribe.

A preocupação sobre este tema ocorre tanto das organizações privadas, como nas governamentais. O assunto dentro do governo federal brasileiro vem crescendo desde o ano 2000, quando foi criado o Comitê Gestor da Segurança da Informação, que assessora a Secretaria Executiva do Conselho de Defesa Nacional, na consecução das diretrizes da Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos nesse Decreto (GSI, 2010).

Associada às iniciativas da Presidência da República, em 2007 foi proposto pelo próprio Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República - DSIC, a criação de núcleos de segurança da informação em órgãos federais (RNP, 2010).

Além do DSIC, o Tribunal de Contas da União (TCU), através da Secretaria de Fiscalização de Tecnologia da Informação (SEFTI), tem acompanhado a evolução do tema Segurança da Informação em órgãos públicos. Dos órgãos consultados em 2007 e 2010, nota-se uma evolução positiva para o item segurança da informação, na adoção de boas práticas e normas internacionais, como pode ser visualizado graficamente na Figura 1. Entretanto outros itens sofreram perdas significantes.

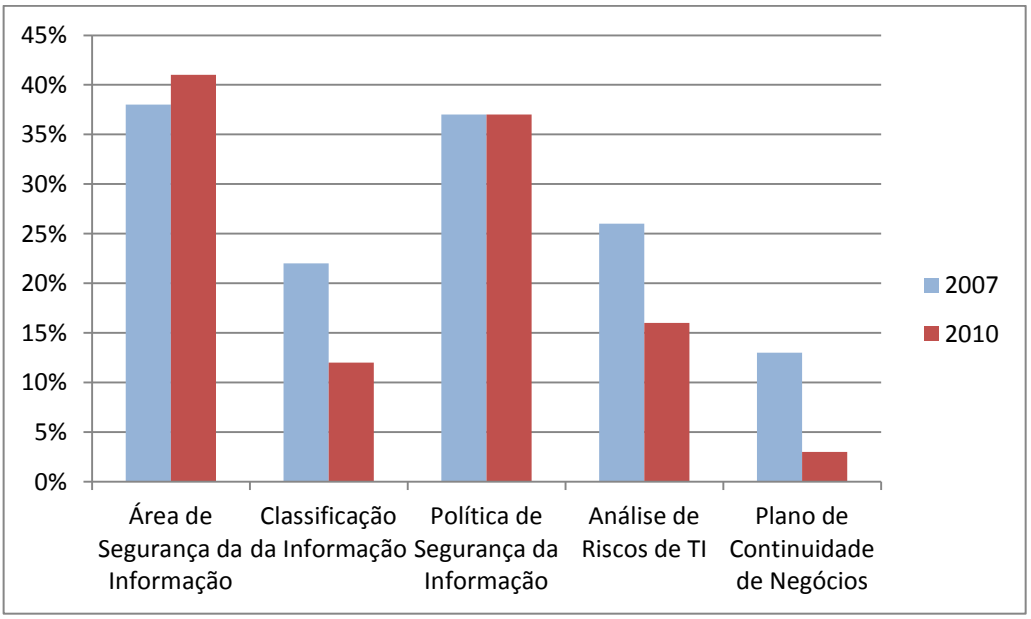

Figura 1: Evolução dos temas pesquisados em Segurança da Informação nos órgãos públicos.
Fonte: TCU, 2010

Com base nestas informações é possível identificar que o tema Segurança da Informação na Administração Pública Federal continua a ser desconhecido, uma vez que os indicadores apresentados na Figura 1 mostram pouca ou nenhuma melhora percentual (apenas três pontos percentuais de melhoria em três anos). A conclusão do TCU (TCU, 2010) sobre esta pesquisa é que as informações críticas não são protegidas adequadamente, assim como não há avaliação de riscos, nem ao menos é possível estimar as suas consequências caso estes se materializem. Para contornar estas dificuldades em tratar a Segurança da Informação, Johnson e Pinto (2010) propuseram um programa de Segurança da Informação para Autarquias Federais em seu trabalho no III Congresso Tecnológico InfoBrasil. Neste trabalho já existe a estruturação da área e das ações de Segurança da Informação com o objetivo de organizar e adequar as autarquias federais no que diz respeito a aderência às boas práticas internacionais.

Em sua pesquisa sobre maturidade da governança da segurança de informação, Britto (2011) destaca o pouco uso de normas e boas práticas como referencia no tratamento de Segurança da Informação de maneira a afetar o desempenho dos produtos e serviços providos pelos órgãos da administração pública direta.

Esta pesquisa apresenta o desenvolvimento de uma proposta de análise de maturidade dos processos de Segurança da Informação com base na norma ABNT NBR ISO/IEC 27002:2005. Esta proposta tem por finalidade se tornar uma ferramenta de avaliação dentro das organizações públicas e privadas, uma vez que tem como base uma norma, auxiliando-as a tratar o tema Segurança da Informação e o quanto este tratamento está alinhado com a principal referência que é o código de boas práticas em segurança da informação, representado pela norma ABNT NBR ISO/IEC 27002:2005.

A estrutura da pesquisa permite que o leitor encontre neste capítulo o tema, problema, objetivos e justificativa do trabalho. No Capítulo 2 encontra-se o referencial teórico utilizado como base na pesquisa. No Capítulo 3 estão descritos os procedimentos metodológicos utilizados para a elaboração dos processos, modelos de maturidade e do questionário. No Capítulo 4 são apresentados os resultados obtidos por meio da execução dos procedimentos metodológicos. No Capítulo 5 são

apresentadas as análises dos resultados, com a discussão da variação da maturidade medida na aplicação do questionário, as considerações finais e a sugestão de trabalhos futuros.

1.1 Tema.

Proposta de uma estrutura de análise de maturidade dos processos de Segurança da Informação com base na norma ABNT NBR ISO/IEC 27002:2005.

1.2 Problema

A Segurança da Informação tem sido tratada nas organizações através da adoção de várias metodologias e normas. Muitas vezes esta combinação de recursos não tem representado o verdadeiro esforço em seguir padrões ou boas práticas, nacionais ou internacionais. O principal problema identificado é: como avaliar a Segurança da Informação de uma organização de forma estruturada, com base na norma ABNT NBR ISO/IEC 27002:2005, a fim de que esta mesma organização possa identificar as principais lacunas que necessitam de tratamento específico no alcance de suas metas de Segurança da Informação?

1.3 Objetivo Geral

- Desenvolver uma estrutura de análise de maturidade que possa oferecer a uma organização uma comparação de suas ações e iniciativas de segurança da informação com os processos padrões estabelecidos pela norma ABNT NBR ISO/IEC 27002:2005.

1.4 Objetivos Específicos

- Propor uma estrutura de processos que representem os objetivos de controle estabelecidos na norma ABNT NBR ISO/IEC 27002:2005;
- Desenvolver os modelos de maturidade para os trinta e nove processos que contemplem os objetivos de controle da norma ABNT NBR ISO/IEC 27002:2005, seguindo o modelo CMMI (*Capability Maturity Model Integration*);

- Desenvolver uma ferramenta computacional (sistema de informações) para a aplicação do questionário que avalie a maturidade da segurança da informação de uma organização, conforme os processos e os modelos de maturidades propostos;
- Validar a ferramenta e a metodologia através da aplicação da avaliação de maturidade da segurança da informação.

1.5 Justificativa

A segurança da informação tem sido um assunto cada vez mais discutido dentro das organizações (BAARS *et al.*, 2009). Mas a abordagem da segurança da informação ainda possui muita influência das ações de segurança de rede executadas pelas áreas de infraestrutura da área de Tecnologia da Informação das organizações (MARCIANO, 2006).

Muitas das atividades executadas possuem caráter corretivo e pouco alinhamento com as reais necessidades que o negócio da organização demanda. Além disso, as atividades são executadas conforme os problemas acontecem, e por vezes, influenciam outras ações já realizadas, aumentando as vulnerabilidades e, principalmente, potencializando os riscos de Segurança da Informação.

Por outro lado, os riscos de Segurança da Informação geralmente não possuem um processo definido e seguido, até porque existe uma confusão no entendimento do conceito de risco, ameaça e vulnerabilidade (TCU, 2010). A matriz de risco, quando executada, tem a tendência de atender a requisitos de operação de TI, como o ambiente de Datacenter, Firewall e Antivírus, mas não consegue abordar outras áreas que influenciam diretamente a Segurança da Informação, como recursos humanos, segurança física, treinamentos, conscientização.

Com o crescimento da utilização da TI nas organizações produziram-se formas de alinhamento da mesma às estratégias de negócio e controle de informações (BYTHEWAY, 2011), porém não necessariamente ligando-a as boas práticas de segurança, sugeridos pelas normas nacionais e internacionais.

Por fim, mesmo as organizações que possuem uma segurança da informação mais aderente à norma ABNT NBR ISO/IEC 27002:2005 (antigamente conhecida

como ISO 17799) (MARCIANO, 2006), não conseguem medir, de forma única e objetiva, seu desempenho e maturidade. A falta destas medições inibe a geração de indicadores precisos, que apoiem a tomada de decisão (de investimentos, recursos e diretrizes), assim como impossibilita a comparação da Segurança da Informação com outras organizações.

Tomando como base estas informações, a utilização de uma estrutura de trabalho para o contexto da Segurança da Informação com base em uma norma internacional específica pode ser útil. Seguindo tendência internacional de adotar o arcabouço do COBIT (*Control Objetives for Information and Related Technology*) (ITGI, 2008) para apoiar a Governança da Tecnologia da Informação, é possível vislumbrar sua adaptação com a norma ABNT NBR ISO/IEC 27002:2005 (código de boas práticas em Segurança da Informação) e como resultado obter um modelo de análise de maturidade de processos, específico para o tratamento da Segurança da Informação.

Desta forma, pretende-se com este trabalho contribuir para os estudos da gestão da Informação, ao mesmo tempo fornecendo base teórico-prática para avaliação do nível de maturidade em segurança da informação às organizações, unindo-se e divulgando conceitos oriundos da Ciência da Informação, da Tecnologia da Informação e da Gestão da informação nas organizações. Em suma, pretende-se sugerir forma de implementar a pró-atividade na gestão da segurança. Contrapondo a realidade reativa encontrada nesta pesquisa e na literatura pesquisada.

2 REFERENCIAL TEÓRICO

A informação é considerada um ativo dentro das organizações, sendo essencial para os processos de negócios e por isso precisa ser protegida adequadamente. Ativo é qualquer coisa que tenha valor para a organização, tendo ou não referência financeira, ou seja, o ativo pode ter um valor financeiro e/ou um valor intangível para o negócio (ABNT, 2005).

A informação existe nas mais diversas formas, como informação impressa, eletrônica, falada. A segurança da informação é a proteção da informação, sob os mais variados aspectos, minimizando suas vulnerabilidades e as ameaças relacionadas. Mais objetivamente, é a preservação da confidencialidade, integridade e disponibilidade da informação (ABNT, 2005).

A vulnerabilidade de um ativo é um fator intrínseco, ou seja, ela vai existir sob qualquer circunstância e pode ser entendida como uma fragilidade que pode ser explorada por uma ou mais ameaças (ABNT, 2005). Uma característica da vulnerabilidade é a sua conotação negativa, que remete ao entendimento de falha e/ou erro.

Por outro lado, as ameaças existem nas mais diversas formas e é a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. Um incidente é um ou uma série de eventos indesejados ou inesperados, que tenham ocorrido em um ativo da informação e que possa comprometer sua confidencialidade, integridade, disponibilidade e que esteja em desacordo com as políticas de seguranças da informação da organização (ABNT, 2005).

O risco é a combinação da probabilidade e o impacto de uma ameaça explorar uma ou mais vulnerabilidades (ABNT, 2005). A maneira de controlar os riscos de segurança da informação é através de uma matriz de riscos. A matriz de riscos é a forma de identificar quais vulnerabilidades um ativo possui, quais são as ameaças que podem explorar estas vulnerabilidades, quais são os impactos caso uma ameaça explore uma vulnerabilidade e quais são as probabilidades disto ocorrer. A partir da matriz de riscos é possível identificar os de níveis mais altos e definir controles específicos para mitigá-los (ABNT, 2005).

Para fazer segurança da informação são utilizados vários tipos de métodos como controles, políticas, processos e procedimentos. A aplicação destes métodos visa mitigar os riscos aos quais a informação está exposta devido a sua natureza. Um controle também pode ser entendido como uma proteção ou contramedida (ABNT, 2005).

Um dos primeiros passos para tratar a segurança da informação dentro de uma organização é a definição de uma política de segurança da informação (BAARS *et al.*, 2009). Uma politica de segurança da informação representa as intenções e diretrizes globais formalmente expressas pela alta gestão de uma organização (ABNT, 2005).

A Segurança da Informação tem sido entendida como uma deficiência dentro das organizações, geralmente relacionada a riscos, ameaças, vulnerabilidades e com uma conotação negativa (BAARS *et al.*, 2009). As primeiras abordagens de segurança foram relacionadas à segurança de redes, principalmente no início do uso da Internet. Hoje, as organizações já compreendem que a segurança saiu dos limites da Tecnologia da Informação, atingindo todo o ambiente corporativo.

A preocupação em tratar a Segurança da Informação de forma homogênea, com base nas melhores práticas internacionais, levou a criação de normas internacionais específicas, como a norma britânica BS 7799:2000, que hoje é conhecida internacionalmente como ISO/IEC 27002:2005 e nacionalmente como ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005). Além disso, a Segurança da Informação também é abordada em boas práticas de Gestão de Serviços de TI, como a Biblioteca ITIL - *Information Technology Infrastructure Library* (ITSMF, 2010), e em estruturas de controle como o COBIT (*Control Objectives for Information and Related Technology*) (ITGI, 2008).

2.1 As origens da norma ABNT NBR ISO/IEC 27002:2005

ISO/IEC 27002:2005, a última versão do padrão ISO, com o título completo de “Tecnologia da Informação – Técnicas de Segurança – Código de Práticas para Gerenciamento da Segurança da Informação" é um padrão de aceitação internacional de normas de boas práticas para a segurança da informação (ABNT,

2005). Para chegar ao estado atual, a norma passou por uma evolução de códigos utilizados em países específicos evoluindo através de novas necessidades muitas vezes oriundas de novas tecnologias, até ser apresentada como uma norma generalista, orientada pela ISO/IEC (BSI, 2010).

O primeiro código de boas práticas foi publicado em 1993 pelo NCC – *National Computing Center* do Reino Unido (NCC, 2011). A partir destas boas práticas foi desenvolvido o Código de Práticas para Gerenciamento da Segurança da Informação, como um padrão Britânico oficial; na verdade, o BS 7799 é, de fato, pré-versão do *Departament of Trade and Industry* (DTI), de 1993 (BSI, 2010). Já em 1995 foi lançada a norma BS 7799:1995 pelo British Standards Institute - BSI, o Instituto Britânico BSI de Padrões, agora conhecido como BSI Padrões Britânicos (BSI British Standards), que faz parte do BSI Group (BSI, 2010). Em 1999 foi publicada a prévia do padrão britânico 7799, então parte 2, que mais tarde seria chamado de ISO/IEC 27001, padrão de certificação em segurança de informação. Assim, o padrão original do código de boas práticas foi renomeado como ‘parte 1’ (BSI, 2010). Após o ciclo de análises e revisões, a BS 7799 foi adaptada pela ISO/IEC e foi publicada como ISO/IEC 17799, em dezembro de 2000 (BSI, 2010). Em junho de 2005, a versão 2000, foi novamente revisada, com novas seções de conselhos consolidados em risco e gerenciamento de incidentes. Com uma estruturação nova e dotada de seções, sendo formalmente publicada a norma ISO/IEC 27002:2005 (ABNT, 2005).

Mas o alinhamento de controles de uma norma dentro do ambiente corporativo precisa estar dentro do alinhamento estratégico, com entrega de valor, gestão de riscos e recursos e, principalmente, monitorada e avaliada. Estes são os princípios básicos da Governança de Tecnologia da Informação proposto pelo COBIT em sua versão 4.1 (ITGI, 2008). A Governança está focada no negócio da organização e como a TI - Tecnologia da Informação está suportando os processos de negócio através de processos de TI definidos. Com base nestes princípios de Governança, as organizações passaram a tratar a Tecnologia da Informação como um parceiro estratégico, com orientação ao negócio.

2.2 A governança da tecnologia da informação

> A governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização. (ITGI, 2008, p. 7).

Este tratamento é muito mais completo e complexo do que a antiga visão de que a Tecnologia da Informação era apenas um provedor de infraestrutura e serviços. As organizações que alcançaram a Governança da Tecnologia da Informação podem facilmente avaliar o retorno de investimento dentro desta área, assim como comparar seu desempenho com outras organizações que utilizaram o mesmo *framework* (ITGI, 2008).

A estrutura que suporta a adoção e implementação de um modelo de governança de TI é o COBIT (CORRÊA, 2006). O COBIT propõe o relacionamento dos objetivos de negócio de uma organização com os processos de TI que suportam a mesma. Desta forma foi elaborado um conjunto de relações entre requisitos de negócios, recursos de TI e processos de TI. Isso é representado pelo cubo do COBIT, como pode ser visualizado na Figura 2.

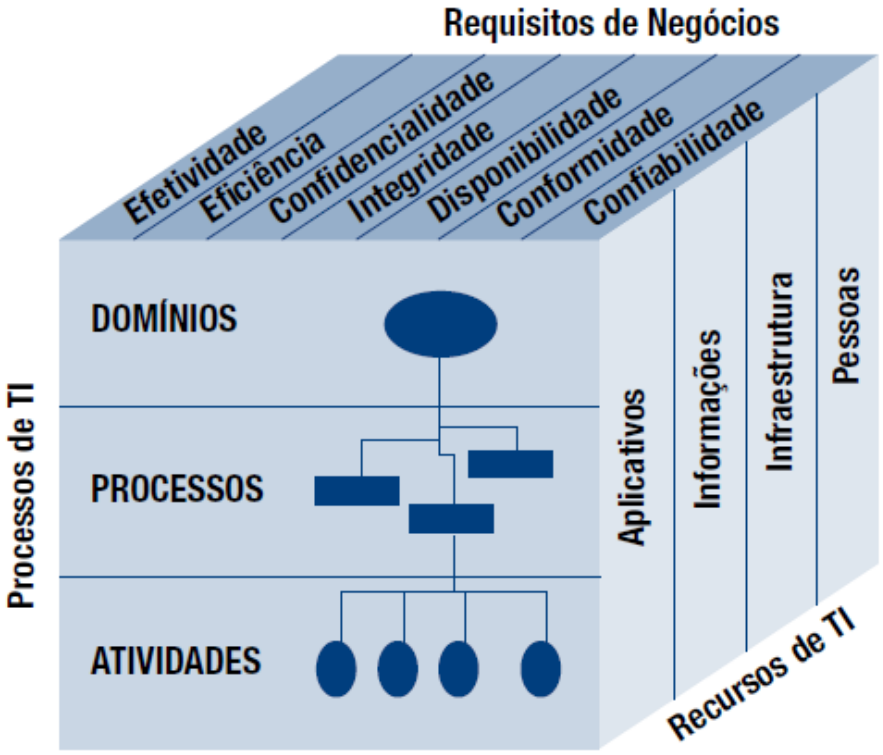

Figura 2 - Representação do cubo do COBIT
Fonte: ITGI, 2008

Os objetivos de negócios são atendidos pelos requisitos de negócio, definidos pelo COBIT como (ITGI, 2008): a) Efetividade - lida com a informação relevante e pertinente para o processo de negócio bem como a mesma sendo entregue em tempo, de maneira correta, consistente e utilizável; b) Eficiência - relaciona-se com a entrega da informação através do melhor (mais produtivo e econômico) uso dos recursos; c) Confidencialidade - está relacionada com a proteção de informações confidenciais para evitar a divulgação indevida. d) Integridade - relaciona-se com a fidedignidade e totalidade da informação bem como sua validade de acordo os valores de negócios e expectativas; e) Disponibilidade - relaciona-se com a disponibilidade da informação quando exigida pelo processo de negócio hoje e no futuro. Também está ligada à salvaguarda dos recursos necessários e capacidades associadas; f) Conformidade - lida com a aderência a leis, regulamentos e obrigações contratuais aos quais os processos de negócios estão sujeitos, isto é, critérios de negócios impostos externamente e políticas internas; g) Confiabilidade - relaciona-se com a entrega da informação apropriada para os executivos para administrar a entidade e exercer suas responsabilidades fiduciárias e de governança.

Por outro lado, os recursos de TI identificados no COBIT podem ser definidos como segue (ITGI, 2008): a) Aplicativos - são os sistemas automatizados para usuários e os procedimentos manuais que processam as informações; b) Informações - são os dados em todas as suas formas, a entrada, o processamento e a saída fornecida pelo sistema de informação em qualquer formato a ser utilizado pelos negócios; c) Infraestrutura - refere-se à tecnologia e aos recursos (ou seja, hardware, sistemas operacionais, sistemas de gerenciamento de bases de dados, redes, multimídia e os ambientes que abrigam e dão suporte a eles), que possibilitam o processamento dos aplicativos; d) Pessoas - são os funcionários requeridos para planejar, organizar, adquirir, implementar, entregar, suportar, monitorar e avaliar os sistemas de informação e serviços. Eles podem ser internos, terceirizados ou contratados, conforme necessário.

O COBIT define as atividades de TI em um modelo de processos genéricos com quatro domínios. Esses domínios são Planejar e Organizar, Adquirir e Implementar, Entregar e Suportar e Monitorar e Avaliar. Esses domínios mapeiam as

tradicionais áreas de responsabilidade de TI de planejamento, construção, processamento e monitoramento.

Com estes relacionamentos, o COBIT suporta a governança de TI provendo uma metodologia para assegurar que: A área de TI esteja alinhada com os negócios; A área de TI habilite o negócio e maximize os benefícios; Os recursos de TI sejam usados responsavelmente; Os riscos de TI sejam gerenciados apropriadamente; Mensurar o desempenho de TI. Para isso, o COBIT possui um diagrama conhecido como o diamante da governança, como pode ser visualizado na Figura 3. Este diagrama representa as cinco áreas foco da governança de TI e cada processo do COBIT deve estar alinhado a, pelo menos, uma destas áreas. Desta forma, é possível entender como cada processo COBIT contribui para a governança de TI.

Figura 3 - Diamante do COBIT
Fonte ITGI, 2008.

As áreas foco são definidas pelo ITGI (2008) como: a) Alinhamento estratégico - foca em garantir a ligação entre os planos de negócios e de TI, definindo, mantendo e validando a proposta de valor de TI, alinhando as operações de TI com as operações da organização; b) Entrega de valor - é a execução da proposta de valor de TI através do ciclo de entrega, garantindo que TI entrega os prometidos benefícios previstos na estratégia da organização, concentrando-se em

otimizar custos e provendo o valor intrínseco de TI; c) Gestão de recursos - refere-se à melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI: aplicativos, informações, infraestrutura e pessoas. Questões relevantes referem-se à otimização do conhecimento e infraestrutura; d) Gestão de risco - requer a preocupação com riscos pelos funcionários mais experientes da corporação, um entendimento claro do apetite de risco da empresa e dos requerimentos de conformidade, transparência sobre os riscos significantes para a organização e inserção do gerenciamento de riscos nas atividades da companhia; e) Mensuração de desempenho - acompanha e monitora a implementação da estratégia, término do projeto, uso dos recursos, processo de desempenho e entrega dos serviços, usando, por exemplo, "*balanced scorecards*" que traduzem as estratégias em ações para atingir os objetivos, medidos através de processos contábeis convencionais.

Em organizações que possuem a maturidade dos negócios mais avançada, os sistemas de informação e mesmo a governança da própria tecnologia da informação serão tratados como requisitos para a governança corporativa (BYTHEWAY, 2011). A relação entre a governança de tecnologia da informação e a governança corporativa ajuda a gerenciar a relação com os acionistas, assim como gerenciar o desempenho das áreas de negócio e a complexa estrutura de tecnologia de informação que o suporta.

Uma das principais mudanças que ocorreram dentro da área da Tecnologia da Informação, das organizações que implantaram a Governança de TI, é a abordagem das demandas de serviços como Projetos de TI (PMI, 2010), orientados às boas práticas de gerenciamento de projetos baseadas no *Project Management Institute* - PMI (PMI, 2010).

Dentro deste cenário de controle, monitoramento, avaliação de desempenho e alinhamento, é possível identificar várias iniciativas com o objetivo de prover uma estrutura que apóie a organização a realizar a Governança da Segurança da Informação. O guia de Governança da Segurança da Informação para os Gerentes de Segurança, proposto pelo ITGI (2008) e o estudo de "Um modelo para inclusão da governança da segurança da informação no escopo da governança organizacional" de Bernardes e Moreira (2005), discutem um modelo para esta

abordagem, concluindo pela necessidade do desenvolvimento formal de uma estrutura (*framework*), que possa ser seguida para a implementação da Governança da Segurança da Informação. Esta estrutura formal deve contemplar a especificação de objetivos de controle documentados, assim como processos, atividades e modelos de avaliação de maturidade.

As organizações buscam alcançar a perfeição, até mesmo um grande desempenho para poder se manter no mercado (SIQUEIRA, 2010). Para a empresa atingir a essa meta de crescimento do negócio é fundamental que ela faça uma análise de maturidade. É um conceito utilizado para ajudar as empresas com o processo de organizar.

Tão importante quanto chegar a algum lugar, é necessário saber em que grau de maturidade a organização está, aplicando um questionário para os gerentes, e pela avaliação das respostas, chegar ao nível de amadurecimento que a empresa precisa por meio de ações de melhoria. Segundo Siqueira (2010), as empresas que fazem esse processo para medir a maturidade acabam crescendo, evoluindo para um grau mais elevado.

Por meio da análise de maturidade dos processos de TI é possível identificar pontos de melhoria nestes processos. A partir disto, desenvolver um planejamento estratégico de melhoria, estabelecendo-se o caminho para atingir novos níveis desejados de maturidade. O plano busca trabalhar sobre os pontos fortes (reforçando-os) e fracos (mitigando-os) que precisam ser melhorados e traçar o planejamento a ser alcançado (SIQUEIRA, 2010). Esses procedimentos dependem de uma integração todas as pessoas da organização alinhadas com o objetivo corporativo.

Para poder abordar a maturidade de processos, é importante que a organização trabalhe sob a ótica da gestão de processos, pois além de aumentar a organização, os processos são o insumo das principais metodologias de gestão e melhorias utilizadas pelas organizações.

2.3 Gestão por Processo

Rafael Santos (2007) argumenta que a gestão por processos tem se tornado peça fundamental nas organizações devido a sua capacidade de contribuir para superar as limitações dos modelos funcionais atuais. Neste sentido, a melhoria em uma operação ou procedimento se torna maior quando este é realizado sob a estrutura de um processo.

A visão de gestão por processos geralmente nos remete a um cenário da engenharia de produção, focada em processos industriais e seguida de exemplos fortes como o Sistema Toyota de Produção (ANTUNES JÚNIOR, 2006). Esta visão faz com que as organizações pensem em industrializar sua operação, independente de ser uma indústria, e fazer com que as suas atividades sejam repetíveis, melhoráveis, gerenciáveis e principalmente controladas.

A capacidade de gerenciamento de uma organização pode ser relacionada a dois pontos: a existência de processos e o nível de maturidade desses processos. O foco em processos do COBIT é um exemplo como prover a governança de TI através da sistematização de atividades, seu controle e principalmente sua aferição (ITGI, 2008). Conceitos de arquitetura corporativa ajudam a identificar os recursos essenciais para o sucesso dos processos: aplicativos, informações, infraestrutura e pessoas (itens que fazem parte do cubo do COBIT). Em resumo, é importante que os processos forneçam as informações de que a empresa necessita para atingir seus objetivos, gerenciando adequadamente seus recursos e medindo seu desempenho.

Outro ponto importante na adoção de um processo é o seu ciclo de melhoria, como, por exemplo, o ciclo de PDCA. Todas as definições apresentadas para o termo “administrar” regem uma sequência de atividade a serem realizadas para que a empresa atinja seus objetivos. A ideia de sequência de atividades está contida na estrutura do ciclo PDCA. O ciclo PDCA é descrito como “uma ferramenta que orienta a sequência de atividades para se gerenciar uma tarefa, processo, empresa, etc.” (MOURA, 1997). O ciclo PDCA está fundamentado nos conceitos de administração, amplamente divulgados e estudados, tornando-o fácil de ser compreendido (ANDRADE, 2003).

No próprio texto da norma NBR ISO 9001:2000 (ABNT, 2001), faz-se referência à utilização do método de melhorias PDCA como forma de gerenciar processos. Sendo assim, as normas ISO 9000 descrevem o ciclo PDCA como parte integrante do seu Sistema de Gestão de Qualidade.

Existem outras maneiras de fazer a melhoria contínua de processos, como a que deriva da expressão japonesa *Kaizen*. A palavra *Kaizen* pode ser entendida com *Kai*–mudança e *Zen*–bom, ou seja, mudança para melhor. Segundo Tessari (IMAI, 1988 *apud* TESSARI, 2008) significa melhoramento contínuo, envolvendo todos na organização. Sendo o *Kaizen*, um estado de melhoria contínuo, em sua essência permeia vários sistemas de gestão, como o TPM (*Total Productive Maintenance*), JIT (*Just-in-time*) e TQC (*Total Quality Control*). Outra metodologia que fornece apoio à identificação de pontos de melhoria é o uso do diagrama de causa e efeito, conhecido como Diagrama de Ishikawa (MASSOCO, 2008), por ser uma ferramenta simples, flexível, de fácil utilização e que pode abordar qualquer tipo de problema onde se busque uma causa raiz, pois relaciona uma característica de qualidade (efeitos) e os seus fatores (causas).

Mas, além de realizar os processos, a organização precisa estar preocupada em como os realizá-los. Esta análise qualitativa da execução de processo faz referência ao grau de eficiência que a organização possui no processo (SILVA, 2009). Para avaliar a maturidade de um processo é necessário escolher um modelo de análise de maturidade.

A análise de maturidade é o ato de avaliar a maturidade de um processo, ou seja, tomando como base o modelo de maturidade de um processo, analisar em qual nível este processo se encontra em uma organização (FERNANDES e ABREU, 2008).

2.4 Maturidade de Processo

O modelo de maturidade de processo foi criado a partir de 1991 pelo SEI (*Software Engineering Institute*) com o objetivo de avaliar a qualidade de um software a partir do seu processo de desenvolvimento (FERNANDES e ABREU, 2008). A partir deste modelo, vários outros foram criados buscando atender as

necessidades do mercado de tecnologia da informação, sendo que em 2002 o SEI criou o CMMI (*Capability Maturity Model Integration*), atualmente o mais utilizado modelo de análise de maturidade de processo existente e o mais adaptável a qualquer tipo de processo.

Segundo Silva (2009), para aperfeiçoar constantemente seus processos, uma organização precisa alcançar altos níveis de maturidade nos mesmos. Esta maturidade precisa ser baseada em políticas para poder conduzir o sucesso da administração e gestão das organizações. Quanto mais efetivo e eficaz um processo, maior é seu nível de maturidade.

O uso de modelos de maturidade em Tecnologia da Informação foi mais intenso a partir do momento que estruturas de governança corporativa de TI foram sendo desenvolvidas e se baseavam na gestão de processos. Estas estruturas comparavam as empresas através da maturidade dos processos que elas possuíam. A principal estrutura de governança utilizada no mundo é o COBIT (ITGI, 2008) e seus processos são avaliados seguindo o modelo de maturidade genérico derivado do CMMI. O modelo de maturidade para o gerenciamento e controle dos processos de TI do COBIT é baseado num método de avaliar a organização, permitindo que ela seja pontuada em uma escala que varia de 0 a 5, sendo o nível de maturidade não-existente igual a zero (0), e o nível de maturidade otimizado igual a cinco (5).

Silva (2009) lista trinta modelos de maturidade existentes, em diversas áreas de conhecimento, sendo que o mais referenciado (adaptado) é o modelo do CMMI.

No COBIT, é fornecido um modelo genérico de maturidade que é interpretado de acordo com a natureza dos processos de gerenciamento de TI. Independente do modelo de maturidade sugere-se que as escalas não devem ser tão granulares, como, por exemplo, 1,15, o que acrescentaria uma visão subjetiva da interpretação do processo, o que foge do propósito de se identificar onde precisa-se de ações de melhorias (FERNANDES e ABREU, 2008). No Quadro 1 é apresentado o modelo de maturidade genérico derivado do CMMI e utilizado pelo COBIT (ITGI, 2008).

0 Não existente quando Completa falta de um processo reconhecido. A empresa nem mesmo reconheceu que existe uma questão a ser trabalhada.
1 Inicial/Ad Hoc quando 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 mas intuitivo quando 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 deixada com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e consequentemente erros podem ocorrer.
3 Definido quando 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 quando A gerência 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 quando 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.

Quadro 1: Modelo de maturidade genérico do CMMI.
Fonte: ITGI, 2008.

Mesmo se o modelo de maturidade seguir uma escala linear de 0 a 5, os diferentes níveis de maturidade exigem graus de complexidade distintos (CAROSIA, 2004). A dificuldade em se alcançar tais níveis depende do contexto da organização que busca a melhoria. Esse contexto também está relacionado a cultura organizacional.

Carosia (2004) avalia que se uma organização inicia do nível 1, é bem provável que achará o nível 2 muito difícil, pois isso incide em uma adoção de gestão por processos e a mudança da cultura organizacional. A partir deste ponto o

desafio está mais relacionado a complexidade do que com a cultura. A organização e planejamento aumentam junto com o nível de maturidade (Figura 4). Conforme sugerido nos traços verticais, da Figura 4, se conseguir atingir o nível 2 é bem provável que considere os níveis sucessivos mais fáceis. Os programas de melhoria são mais eficientes a partir deste ponto.

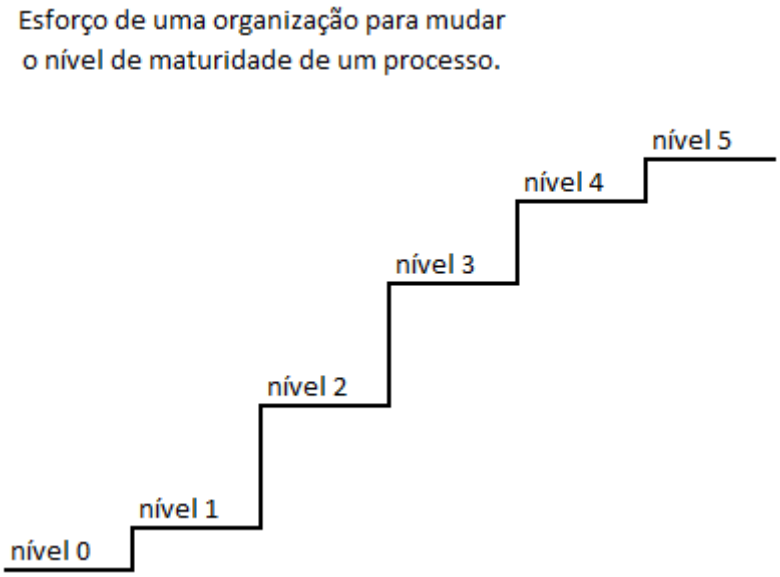

Figura 4 - Esforço necessário para mudar o nível de maturidade de um processo.
Fonte: CAROSIA, 2004.

3 PROCEDIMENTOS METODOLÓGICOS

Conforme Santos (1999) esta pesquisa classifica-se, segundo seus objetivos, como exploratória, uma vez que se busca maior familiaridade com os componentes da Segurança da Informação. Pelos seus procedimentos de coleta, classifica-se como levantamento, uma vez que se busca junto ao grupo de interesse a avaliação da metodologia proposta.

Os procedimentos metodológicos para a elaboração do trabalho são apresentados na Figura 5 e descritos a seguir. Eles representam a evolução do trabalho, partindo da proposta inicial de abordar a norma ABNT NBR ISO/IEC 27002:2005, até a avaliação dos resultados obtidos através da aplicação do questionário de maturidade da Segurança da Informação.

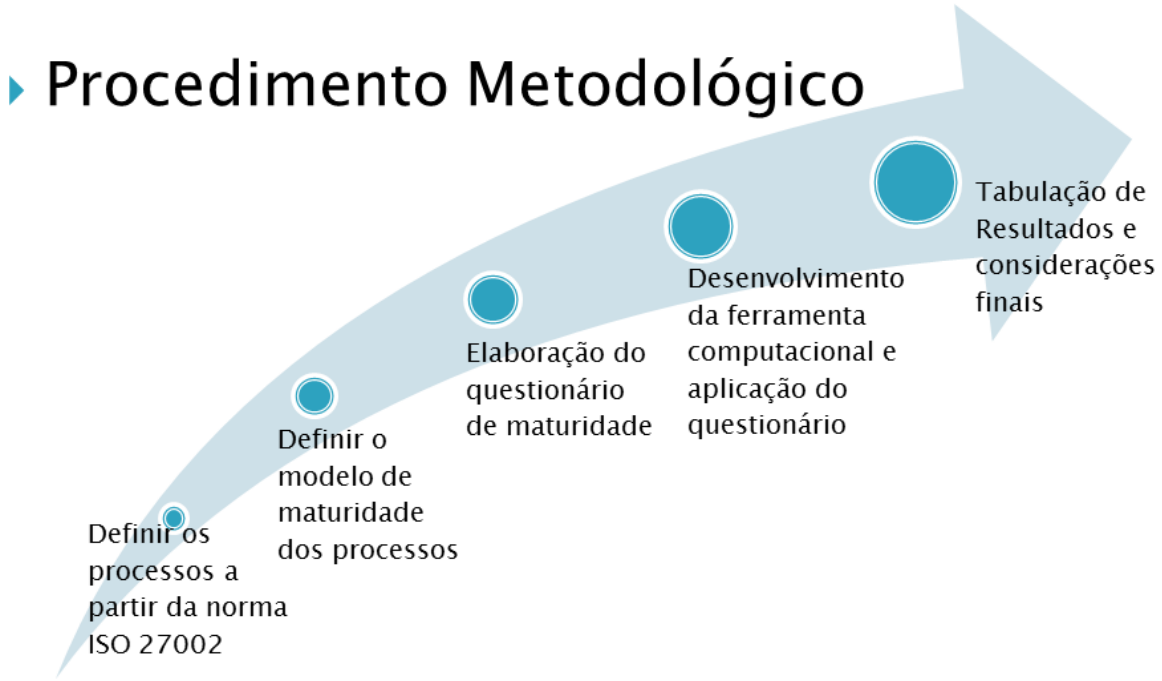

Figura 5 - Apresentação esquemática dos procedimentos metodológicos.
Fonte: O Autor.

3.1 Definir os processos a partir da norma ISO 27002

A primeira fase desta etapa foi a leitura da norma ABNT NBR ISO/IEC 27002:2005. Esta leitura teve como objetivo entender a estrutura da norma e identificar as estruturas que seriam mais adequadas à abordagem da gestão de processos. Partindo do princípio que um processo é composto de atividades internas

específicas, as estruturas candidatas a processos foram os objetivos de controle. A definição dos processos se deu através da adaptação dos objetivos de controle em processos, sendo que seus controles foram interpretados como as atividades necessárias para atingir cada objetivo do processo.

3.2 Definir o modelo de maturidade dos processos

O modelo de maturidade foi definido com base no modelo genérico CMMI (*Capability Maturity Mode Integration*) apresentado na estrutura do COBIT. Este modelo foi adotado por ser flexível a este trabalho, uma vez que é originado em outra área da tecnologia da informação e já existe, como, por exemplo, no COBIT, sua adaptação e interpretação. Para cada processo identificado foi elaborado um modelo de maturidade específico.

3.3 Elaboração do questionário de maturidade

Foi elaborado um questionário de maturidade para cada processo identificado. As questões que compõe cada questionário têm como objetivo avaliar os diversos níveis de maturidade dos processos de segurança da informação. Para cada questão elaborada existem quatro possíveis respostas distribuídas em níveis de abrangência. Cada questão possui uma resposta que indica se aquele processo atingiu ou não os níveis mínimos para os diversos níveis de maturidade. Os processos, modelos de maturidade e questionários propostos estão listados no Apêndice B.

Foram elaboradas quinhentas e noventa e uma (591) questões que abrangem os trinta e nove processos e seus respectivos cinco níveis de maturidade. Para facilitar a aplicação deste questionário foi desenvolvida uma ferramenta computacional (sistema de informações).

3.4 Desenvolvimento da ferramenta computacional e aplicação do questionário

Para que a aplicação do questionário fosse confortável aos respondentes, foi desenvolvida uma ferramenta computacional (sistema de informação). Este sistema, com interface web, foi disponibilizado no endereço eletrônico

http://www.iso27000.com.br/mestrado, onde os respondentes convidados puderam ler as instruções de acesso e proceder ao preenchimento da pesquisa.

O objetivo da ferramenta computacional é o de facilitar ao respondente o preenchimento da pesquisa, oferecendo a comodidade que preenchê-la no momento que achar conveniente, bastando para isso um computador com acesso a Internet e um software de navegação Internet, como, por exemplo, o *Internet Explorer* da Microsoft.

O sistema foi desenvolvido em programação orientada a objeto, utilizando a linguagem de programação PHP - *Hypertext Preprocessor* (PHP, 2011), que é orientada a Web. Ele foi desenvolvido em duas línguas: português e inglês.

Todas as regras do questionário foram aplicadas a ferramenta computacional. Além disso, a tabulação dos dados é realizada automaticamente, exibindo os resultados ao respondente em tempo real. Os resultados são apresentados tanto em modo texto quanto em modo gráfico através de gráficos do tipo radar. No apêndice A é possível visualizar exemplos de telas do sistema. O código fonte do sistema não é apresentado neste trabalho por ser objeto de registro de marcas e patentes, através da Agência de Inovação da Universidade Federal do Paraná.

3.5 Universo

O grupo de respondentes para a pesquisa foi definido como os representantes (gerentes ou diretores de TI) de 10 (dez) empresas da região de Curitiba que possuem mais de 1000 (mil) usuários internos de serviços de TI, representando qualquer área de atividade comercial, assim como de carácter público e privado. Essa definição se deveu ao pouco tempo disponível para a aplicação do questionário, apenas dois meses, associado a pouca disponibilidade dos respondentes e a complexidade e volume de questões. Outro fator limitante para o preenchimento do questionário se deve ao caráter estratégico que as questões de segurança da informação representam para uma organização, uma vez que ao entrar em contato com os respondentes, dois solicitaram a formalização de um acordo de não divulgação (AND).

3.6 Tabulação de resultados

A tabulação dos resultados se deu de maneira automática, uma vez que o próprio sistema de informação apresenta os resultados em tempo real do preenchimento do questionário.

A principal regra adotada para a tabulação dos resultados foi denominada a como “regra do copo de água”, onde para alcançar determinada maturidade, todas as respostas dos níveis anteriores deveriam ser respondidas iguais ou maiores que o critério mínimo definido para cada questão.

O fluxograma apresentado na Figura 6 representa a lógica adotada no preenchimento do questionário.

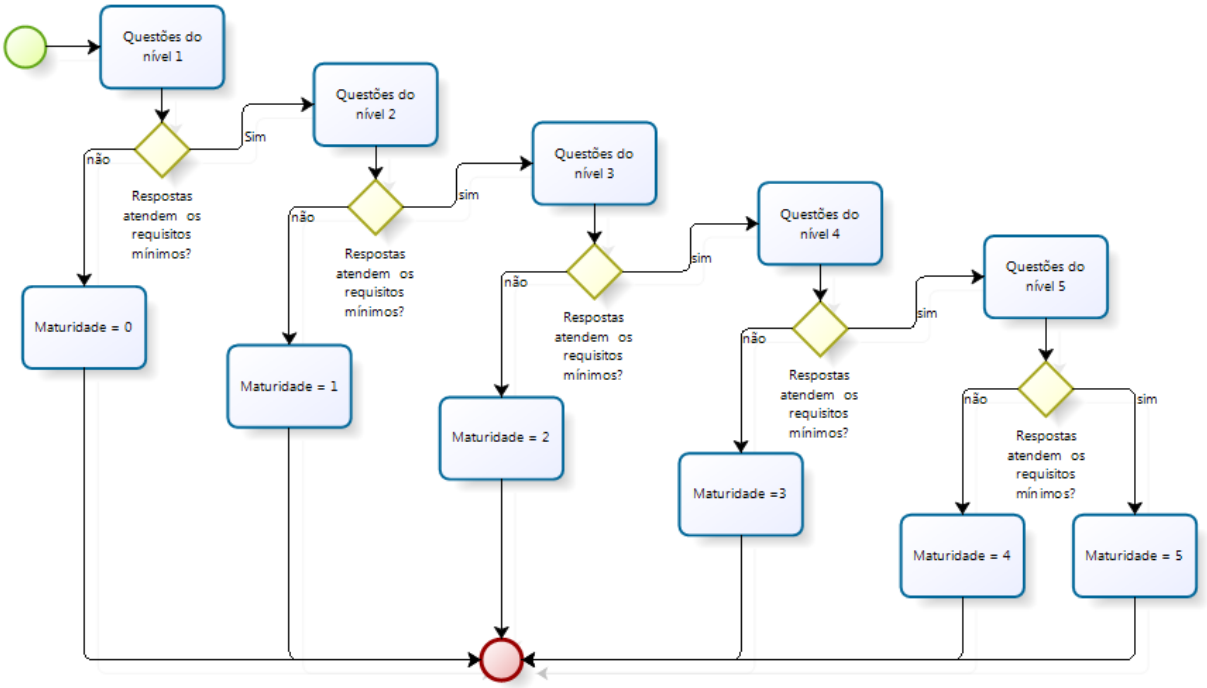

Figura 6 - Fluxograma da lógica do questionário.
Fonte: O Autor.

Neste fluxograma percebe-se que só existe avanço ao nível seguinte caso seja atingido o anterior. Como consequência cada respondente só terá acesso às perguntas correspondentes ao seu nível de maturidade.

3.6.1 Níveis de respostas

Cada questão possui um nível mínimo de resposta (uma alternativa) para que seja considerada a maturidade. Em outras palavras, para cada nível de maturidade avaliado, cada questão possui um nível mínimo de resposta para assegurar que as atividades são executadas dentro da exigência do nível de maturidade avaliado. Desta maneira, caso o respondente assinale uma resposta de nível menor do que a requerida para uma questão, significa que ele não possui o nível de maturidade que está sendo avaliado. Isso assegura que um processo avaliado com determinada maturidade não possua lacunas nas maturidades inferiores.

3.7 Aplicação do questionário

Para aplicação do questionário foram enviados convites através de correio eletrônico, convocando representantes das organizações escolhidas para a participação na pesquisa eletrônica. Em acordo firmado verbalmente com os respondentes, os nomes ou mesmo qualquer tipo de informação das organizações de que eles fazem parte e representam nesta pesquisa não poderiam ser divulgadas.

Este tipo de amostra é conhecido na literatura como amostra por quota, que é o tipo onde o pesquisador entrevista um número predefinido de pessoas em cada uma das várias categorias desejadas (SCHIFFMAN e KANUK, 2000).

3.8 Análise dos resultados

A análise dos resultados, devido a pequena quantidade de respondentes, não possui caráter estatístico e foi realizada com o objetivo de entender: a) qual é a média da maturidade de todos os processos tomando como base todos os respondentes? b) quais são os processos que obtiveram maior e menor média de maturidade? c) Quais são os domínios que apresentam a maior e a menor média de maturidade? d) Quais são os resultados individuais de cada respondente em relação à média da pesquisa para todos os processos? Tais respostas permitirão compreender melhor o tema e encaminhar trabalhos futuros.

3.9 Trabalhos prévios

Esta pesquisa teve origem em outros trabalhos relativos à segurança da informação desenvolvidos ou orientados pelo autor.

O primeiro trabalho sobre o assunto foi apresentado como Trabalho de Conclusão de Curso de Graduação, nas Faculdades ESEEI, em 2008, intitulado “ISO/IEC 27002 – Avaliando o código de boas práticas em segurança da informação e propostas de ferramentas e soluções”, de autoria de Deno Luciano Borges Winkelmann, e de orientação do autor.

O segundo trabalho sobre o assunto foi apresentado III Congresso Tecnológico InfoBrasil, em 2010, intitulado “Proposta de um Programa de Segurança da Informação para as Autarquias Federais”, de autoria de Luciano Johnson e José Simão de Paula Pinto.

O terceiro trabalho relacionado ao assunto foi apresentado como Trabalho de Conclusão de Curso de Graduação, na Faculdade FACEAR, em 2010, intitulado “Proposta de uma estrutura de controle para aderência a norma ABNT NBR 16001:2004”, de autoria de Andressa de Mendonça Pacak, Claudia Regina dos Reis Brandão, Jussara Cristiane Gualdessi e João Maria da Silva, co-orientado, a convite, pelo autor.

4 RESULTADOS

Como apresentado no capítulo 3, o trabalho teve início na identificação dos processos de segurança da informação constantes na norma ISO/IEC 27002:2005. A seguir são apresentados os resultados obtidos de cada fase especificada no procedimento metodológico do trabalho.

4.1 Definição dos Processos

A fase de definição dos processos foi baseada na leitura e interpretação da norma ISO/IEC 27002:2005. Os processos identificados são à base do modelo de maturidade proposto, uma vez que a avaliação de maturidade é realizada por processo. A seguir é apresentado um descritivo das atividades realizadas para a definição dos processos.

4.1.1 Identificação dos processos dentro da estrutura da norma

A norma ISO/IEC 27002:2005 é composta de onze seções. Nestas onze seções estão distribuídos trinta e nove objetivos de controles e nestes estão distribuídos os cento e trinta e três controles de segurança da norma.

A primeira análise realizada foi sobre as onze seções da norma e, teve como objetivo, avaliar se cada seção possuía a estrutura mínima para ser transformada em um processo. Nesta avaliação chegou-se a conclusão que cada seção apenas delimita assuntos de interesse e não está estruturada de maneira a suportar a divisão em atividades específicas requeridas por um processo (entradas-atividades-saídas).

A segunda análise realizada foi sobre os trinta e nove objetivos de controle. Estes objetivos estão estruturados de tal maneira que podem ser transformados em processos, uma vez que possuem atividades internas claramente definidas, assim como entradas e saídas de informações. Estas atividades foram identificadas como sendo os controles de segurança. O Quadro 2 lista os processos identificados a partir da norma ISO/IEC 27002:2005 e que foram tomados como base para a elaboração dos modelos de maturidade propostos neste trabalho.

Planejamento Estratégico da Segurança da Informação
Política de Segurança da Informação
Organização Interna
Organização com as Partes Externas
Gestão de Risco
Responsabilidade pelos Ativos
Classificação da Informação
Segurança em Recursos Humanos
Procedimentos e Responsabilidades Operacionais
Troca de Informações
Requisitos de Negócio para Controle de Acesso
Responsabilidade dos Usuários
Requisitos de Segurança de Sistemas de Informação
Áreas Seguras
Segurança em Equipamentos
Gerenciamento de Serviços de Terceiros
Planejamento e Aceitação dos Sistemas
Proteção contra Códigos Maliciosos e Códigos Móveis
Cópias de Segurança
Gerenciamento da Segurança em Redes
Manuseio de Mídias
Serviços de Comércio Eletrônico
Gerenciamento de Acesso do Usuário
Controle de Acesso a Rede
Controle de Acesso ao Sistema Operacional
Controle de Acesso a aplicação e a Informação
Computação Móvel e Trabalho Remoto
Processamento Correto nas Aplicações
Controles Criptográficos
Segurança dos Arquivos do Sistema
Segurança em Processos de Desenvolvimento e de Suporte
Gestão de Vulnerabilidades Técnicas
Notificação de Fragilidades e Eventos de Segurança da Informação
Gestão de Incidentes de Segurança da Informação e Melhorias
Monitoramento de Atividades
Aspectos da Gestão de Continuidade de Negócios em Segurança da Informação
Conformidade com Requisitos Legais
Conformidade com normas, políticas de Segurança da Informação e Conf. Técnica
Considerações quanto a Auditoria de Sistemas de Informação

Quadro 2 – Listagem dos processos de segurança identificados.
Fonte: O Autor

4.1.2 Categorização dos processos identificados

Uma característica encontrada na análise dos processos é a de categorização. A categorização atua como um agente facilitador no entendimento dos processos e como estes se relacionam. Os processos foram categorizados em

cinco categorias, como é apresentado no Quadro 3. A categorização foi inspirada na estrutura de domínios utilizada pelo COBIT (ITGI, 2008).

POA - Planejamento, Organização e Alinhamento
ORG - Segurança Organizacional
FIS - Segurança Física
TEC - Segurança Técnica
GES - Gestão da Segurança

Quadro 3 – Categorização dos processos de segurança identificados.
Fonte: O Autor

A categoria POA (Planejamento, Organização e Alinhamento) diz respeito aos processos que possuem como objetivo alinhar as iniciativas de segurança da informação com as necessidades e requisitos da operação de negócio da organização. Além disso, também estão incluídos os processos de planejamento de ações e de como a segurança da informação é organizada (estruturada).

A categoria ORG (Segurança Organizacional) diz respeito aos processos que visam à segurança da informação sob a ótica da organização como empresa. Estes processos têm como objetivo organizar as ações de segurança da informação, relacionando os requisitos internos da organização com as práticas de segurança da informação.

A categoria FIS (Segurança Física) diz respeito aos processos que visam à segurança física do ambiente organizacional, também relacionada como segurança patrimonial. Estes processos têm como objetivo prover segurança física em diversos níveis, incluindo a definição de áreas seguras e de acesso restrito. Além disso, a segurança física dos equipamentos também é tratada.

A categoria TEC (Segurança Técnica) diz respeito aos processos de visam à segurança da informação através de atividades específicas de cunho técnico. Estes processos têm como característica serem aplicados aos ambientes de Tecnologia da Informação, onde boa parte dos conceitos de segurança da informação foram analisados e desenvolvidos (BSI, 2010).

A categoria GES (Gestão da Segurança) diz respeito aos processos que visam à gestão da segurança da informação. Estes processos têm por objetivo assegurar as ações de segurança da informação estão organizadas, respondem aos

requisitos de negócio da organização e que estão alinhadas com regulamentos, leis e normas, tanto de caráter interno a organização, como externo.

O Quadro 4 apresenta os processos de segurança e suas respectivas categorias definidas neste trabalho. Para facilitar o tratamento e organização dos processos, foram definidas siglas tanto para as categorias quanto para os processos. Esta definição de siglas foi inspirada na estrutura de processos apresentada pelo COBIT (ITGI, 2008).

POA - Planejamento, Organização e Alinhamento	
	POA01 – Planejamento Estratégico da Segurança da Informação
	POA02 – Política de Segurança da Informação
	POA03 – Organização Interna
	POA04 – Organização com as Partes Externas
	POA05 – Gestão de Risco
ORG - Segurança Organizacional	
	ORG01 – Responsabilidade pelos Ativos
	ORG02 – Classificação da Informação
	ORG03 – Segurança em Recursos Humanos
	ORG04 – Procedimentos e Responsabilidades Operacionais
	ORG05 – Troca de Informações
	ORG06 – Requisitos de Negócio para Controle de Acesso
	ORG07 – Responsabilidade dos Usuários
	ORG08 – Requisitos de Segurança de Sistemas de Informação
FIS - Segurança Física	
	FIS01 – Áreas Seguras
	FIS02 – Segurança em Equipamentos
TEC - Segurança Técnica	
	TEC01 – Gerenciamento de Serviços de Terceiros
	TEC02 – Planejamento e Aceitação dos Sistemas
	TEC03 – Proteção contra Códigos Maliciosos e Códigos Móveis
	TEC04 – Cópias de Segurança
	TEC05 – Gerenciamento da Segurança em Redes
	TEC06 – Manuseio de Mídias
	TEC07 – Serviços de Comércio Eletrônico
	TEC08 – Gerenciamento de Acesso do Usuário
	TEC09 – Controle de Acesso a Rede
	TEC10 – Controle de Acesso ao Sistema Operacional
	TEC11 – Controle de Acesso a aplicação e a Informação
	TEC12 – Computação Móvel e Trabalho Remoto
	TEC13 – Processamento Correto nas Aplicações
	TEC14 – Controles Criptográficos
	TEC15 – Segurança dos Arquivos do Sistema

	TEC16 – Segurança em Processos de Desenvolvimento e de Suporte
	TEC17 – Gestão de Vulnerabilidades Técnicas
GES - Gestão da Segurança	
	GES01 – Notificação de Fragilidades e Eventos de Segurança da Informação.
	GES02 – Gestão de Incidentes de Segurança da Informação e Melhorias
	GES03 – Monitoramento de Atividades
	GES04 – Aspectos da Gestão de Continuidade de Negócios em Segurança da Informação
	GES05 – Conformidade com Requisitos Legais
	GES06 – Conformidade com normas, políticas de Segurança da Informação e Conformidade Técnica
	GES07 – Considerações quanto a Auditoria de Sistemas de Informação

Quadro 4 – As categorias e seus processos identificados.
Fonte: O Autor

4.1.3 Estrutura dos processos identificados

A última etapa para a completa definição dos processos é a apresentação dos processos e suas atividades. As atividades fazem referência aos controles de segurança da informação existentes nos objetivos de controle da norma ABNT NBR ISO/IEC 27002:2005. O Quadro 5 apresenta a estrutura final da definição dos processos.

POA - Planejamento, Organização e Alinhamento	
	POA01 – Planejamento Estratégico da Segurança da Informação
	• Gerenciamento de Valor da Segurança da Informação. • Alinhamento entre Segurança da Informação e Negócio. • Avaliação da Capacidade e Desempenho Correntes. • Plano Estratégico de Segurança da Informação. • Planos Táticos de Segurança da Informação. • Gerenciamento do Portfólio de Segurança da Informação.
	POA02 – Política de Segurança da Informação
	• Elaborar o documento da política de segurança da informação. • Analisar criticamente a política de segurança da informação.
	POA03 – Organização Interna
	• Comprometimento da direção com a segurança da informação. • Coordenação da segurança da informação. • Atribuição de responsabilidades para a segurança da informação.

	• Processo de autorização para os recursos de processamento da informação. • Acordos de confidencialidade. • Contato com as autoridades. • Contato com grupos especiais. • Análise crítica independente de segurança da informação.
POA04 – Organização com as Partes Externas	
	• Identificação dos riscos relacionados com partes externas. • Identificando a segurança da informação, quando tratando com os clientes. • Identificando segurança da informação nos acordos com terceiros.
POA05 – Gestão de Risco	
	• Alinhamento da gestão de riscos de TI e de Negócios. • Estabelecimento do Contexto de Risco. • Identificação de Eventos. • Avaliação de Risco. • Resposta ao Risco. • Manutenção e Monitoramento do Plano de Ação de Risco.
ORG - Segurança Organizacional	
ORG01 – Responsabilidade pelos Ativos	
	• Inventário dos ativos. • Proprietário dos ativos. • Uso aceitável dos ativos.
ORG02 – Classificação da Informação	
	• Recomendações para classificação. • Rótulos e tratamento da informação.
ORG03 – Segurança em Recursos Humanos	
	• Papéis e Responsabilidades. • Seleção. • Termos e condições de contratação. • Responsabilidades da direção. • Conscientização, educação e treinamento em segurança da informação. • Processo disciplinar. • Encerramento de atividades. • Devolução dos Ativos. • Retirada de direito de acesso.
ORG04 – Procedimentos e Responsabilidades Operacionais	
	• Documentação dos procedimentos de operação. • Gestão de mudanças. • Segregação de funções. • Separação dos recursos de desenvolvimento, teste e de produção.
ORG05 – Troca de Informações	
	• Políticas e procedimentos para troca de informações. • Acordos para a troca de informações.

	• Mídias em trânsito. • Mensagens eletrônicas. • Sistemas de informações do negócio.
ORG06 – Requisitos de Negócio para Controle de Acesso	
	• Política de controle de acesso.
ORG07 – Responsabilidade dos Usuários	
	• Uso de senhas. • Equipamento de usuário sem monitoração. • Política de mesa limpa e tela limpa.
ORG08 – Requisitos de Segurança de Sistemas de Informação	
	• Análise e especificação dos requisitos de segurança.
FIS - Segurança Física	
FIS01 – Áreas Seguras	
	• Perímetro de segurança física. • Controles de entrada física. • Segurança em escritórios, salas e instalações. • Proteção contra ameaças externas e do meio ambiente. • Trabalhando em áreas seguras. • Acesso do público, áreas de entrega e de carregamento.
FIS02 – Segurança em Equipamentos	
	• Instalação e proteção do equipamento. • Utilidades. • Segurança do cabeamento. • Manutenção dos equipamentos. • Segurança de equipamentos fora das dependências da organização. • Reutilização e alienação segura de equipamentos. • Remoção de propriedade.
TEC - Segurança Técnica	
TEC01 – Gerenciamento de Serviços de Terceiros	
	• Entrega de Serviços. • Monitoramento e análise crítica de serviços terceirizados. • Gerenciamento de mudanças para serviços terceirizados.
TEC02 – Planejamento e Aceitação dos Sistemas	
	• Gestão de capacidade. • Aceitação de sistemas.
TEC03 – Proteção contra Códigos Maliciosos e Códigos Móveis	
	• Controles contra códigos maliciosos. • Controles contra códigos móveis.
TEC04 – Cópias de Segurança	
	• Cópias de segurança das informações
TEC05 – Gerenciamento da Segurança em Redes	
	• Controles de redes. • Segurança dos serviços de rede.
TEC06 – Manuseio de Mídias	

	• Gerenciamento de mídias removíveis. • Descarte de mídias. • Procedimentos para tratamento de informação. • Segurança da documentação dos sistemas.
TEC07 – Serviços de Comércio Eletrônico	
	• Comércio eletrônico. • Transações on-line. • Informações publicamente disponíveis.
TEC08 – Gerenciamento de Acesso do Usuário	
	• Registro de usuário. • Gerenciamento de privilégios. • Gerenciamento de senha do usuário. • Análise crítica dos direitos de acesso de usuário.
TEC09 – Controle de Acesso a Rede	
	• Política de uso dos serviços de rede. • Autenticação para conexão externa do usuário. • Identificação de equipamento em redes. • Proteção de portas de configuração e diagnóstico remotos. • Segregação de redes. • Controle de conexão de rede. • Controle de roteamento de redes.
TEC10 – Controle de Acesso ao Sistema Operacional	
	• Procedimentos seguros de entrada no sistema (log-on). • Identificação e autenticação de usuário. • Sistema de gerenciamento de senha. • Uso de utilitários de sistema. • Limite de tempo de sessão. • Limitação de horário de conexão.
TEC11 – Controle de Acesso a aplicação e a Informação	
	• Restrição de acesso à informação. • Isolamento de sistemas sensíveis.
TEC12 – Computação Móvel e Trabalho Remoto	
	• Computação e comunicação móvel. • Trabalho remoto.
TEC13 – Processamento Correto nas Aplicações	
	• Validação dos dados de entrada. • Controle do processamento interno. • Integridade de mensagens. • Validação de dados de saída.
TEC14 – Controles Criptográficos	
	• Política para o uso de controles criptográficos. • Gerenciamento de Chaves.
TEC15 – Segurança dos Arquivos do Sistema	
	• Controle de software operacional. • Proteção dos dados para teste de sistema. • Controle de acesso ao código-fonte de programa.
TEC16 – Segurança em Processos de Desenvolvimento e de Suporte	

	• Procedimentos para controle de mudanças. • Análise crítica técnica das aplicações após mudanças no sistema operacional. • Restrições sobre mudanças em pacotes de software. • Vazamento de informações. • Desenvolvimento terceirizado de software.
	TEC17 – Gestão de Vulnerabilidades Técnicas
	• Controle de vulnerabilidades técnicas.
GES - Gestão da Segurança	
	GES01 – Notificação de Fragilidades e Eventos de Segurança da Informação.
	• Notificação de eventos de segurança da informação. • Notificando fragilidades de segurança da informação.
	GES02 – Gestão de Incidentes de Segurança da Informação e Melhorias
	• Responsabilidades e procedimentos. • Aprendendo com os incidentes de segurança da informação. • Coleta de evidências.
	GES03 – Monitoramento de Atividades
	• Registros de auditoria. • Monitoramento do uso do sistema. • Proteção das informações dos registros (log). • Registros (log) de administrador e operador. • Registros (log) de falhas. • Sincronização dos relógios.
	GES04 – Aspectos da Gestão de Continuidade de Negócios em Segurança da Informação
	• Incluindo segurança da informação no processo de gestão da continuidade de negócio. • Continuidade de negócios e análise/avaliação de riscos. • Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação. • Estrutura do plano de continuidade de negócio. • Testes, manutenção e reavaliação dos planos de continuidade do negócio.
	GES05 – Conformidade com Requisitos Legais
	• Identificação da legislação aplicável. • Direitos de propriedade intelectual. • Proteção de registros organizacionais. • Proteção de dados e privacidade de informações pessoais. • Prevenção de mau uso de recursos de processamento da informação. • Regulamentação de controles de criptografia.
	GES06 – Conformidade com normas, políticas de Segurança da Informação e Conformidade Técnica
	• Conformidade com as políticas e normas de segurança da informação.

	• Verificação da conformidade técnica.
GES07 – Considerações quanto a Auditoria de Sistemas de Informação	
	• Controles de auditoria de sistemas de informação. • Proteção de ferramentas de auditoria de sistemas de informação.

Quadro 5: Estrutura dos processos identificados.
Fonte: O Autor.

4.2 Definição do Modelo de Maturidade

O modelo de maturidade de cada processo foi elaborado através do cruzamento do modelo de maturidade genérico proposto pelo CMMI e as atividades definidas para cada processo. O Quadro 6 apresenta o modelo de maturidade genérico adotado pelo CMMI.

Maturidade	Descrição
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 deixada 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 gerência 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

Quadro 6 – Modelo de maturidade genérico do CMMI.
Fonte: ITGI, 2008

Foram elaborados trinta e nove modelos de maturidade, que estão apresentados no apêndice B.

4.3 Questionário de avaliação da maturidade

Para cada modelo de maturidade de processo, foi desenvolvido um questionário de avaliação. Cada questionário possui questões que foram divididas em cinco níveis, representando os níveis de maturidade do processo.

Cada questão possui quatro alternativas de resposta, que representam os níveis em que as atividades de segurança do processo são aplicadas na organização. A norma ABNT NBR ISO/IEC 27002:2005 tem como característica ser aplicada em todas as áreas de qualquer organização (ABNT, 2005). Essa característica inspirou a definição das quatro alternativas de resposta dos questionários: a) somente em algumas situações; b) em toda a tecnologia da informação na organização; c) em vários departamentos da organização, inclusive TI; d) em toda organização.

A alternativa “a) somente em algumas situações” faz referência as atividades de segurança da informação que são executadas somente quando alguma situação exige, ou seja, não é uma atividade rotineira da organização.

A alternativa “b) em toda a tecnologia da informação na organização” faz referência as atividades de segurança da informação que são executadas somente pela área de tecnologia da informação da organização, ou seja, não é uma atividade rotineira das demais áreas da organização.

A alternativa “c) em vários departamentos da organização, inclusive TI” faz referência as atividades de segurança da informação que são executadas em várias áreas da organização, inclusive pela área de tecnologia da informação, ou seja, as atividades de segurança extrapolam o ambiente de tecnologia da informação, abrangendo outras áreas, mas não todas, da organização.

A alternativa “d) em toda organização” faz referência as atividades de segurança da informação que são executadas em todas áreas da organização, demonstrando que o tema segurança da informação é bem evoluído da organização

a ponto de todas as áreas executarem as atividades propostas pelo processo em análise.

A Figura 7 apresenta um exemplo de questões, com as alternativas de respostas e suas respectivas respostas mínimas para atingimento do nível de maturidade.

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
O planejamento da segurança da informação é realizado em resposta a um requisito específico de negócio.		X		
O planejamento estratégico da segurança da informação é discutido nas reuniões da Direção.	X			
O alinhamento de requisitos de negócio, aplicações e tecnologia ocorre de forma reativa..		X		
A segurança da informação se confunde com a segurança de TI.		X		

Figura 7 - Exemplo de questões e respostas do questionário de análise de maturidade.
Fonte: O Autor.

4.4 Ferramenta computacional

O preenchimento da pesquisa demandou um período longo de tempo e, para evitar o desgaste dos participantes, foi possível preenchê-la por etapas. Para acessar a pesquisa, os respondentes receberam um código de acesso pessoal. Este código foi utilizado como chave para acessar o sistema que estava disponível no endereço eletrônico http://www.iso27000.com.br/mestrado. Ao inserir o código de acesso, era apresentada uma tela resumo e a opção de preencher a pesquisa. O preenchimento da pesquisa segue a sequência dos processos definidos, e por isso, se deu através de várias telas. Após preencher as informações de cada tela, o respondente clicava na opção "PRÓXIMO", onde o resultado era armazenado e uma nova tela do questionário era apresentada. Em cada tela existia uma opção "SAIR"

para que o respondente pudesse sair da pesquisa sem finalizá-la ou perder informações. Quando o respondente voltasse à pesquisa, ele era direcionado ao último questionário não finalizado.

Ao chegar à tela final do questionário o respondente era avisado que ele foi finalizado. Na tela principal do sistema existia um gráfico que apresentava o percentual (%) de preenchimento do questionário, assim como os seus resultados e os resultados médios da pesquisa, com gráficos da maturidade medida. Algumas telas do protótipo podem ser vistas no apêndice A.

5 DISCUSSÃO

Uma vez finalizada a etapa de preenchimento dos questionários, o sistema de informação automaticamente tabulou os dados. A análise destes dados, proposta no item 3.6, foi realizada e é apresentada a seguir.

5.1 Média da maturidade de todos os processos

Para se chegar ao valor que representa a média de maturidade de um processo, foi somado o valor individual deste processo para cada respondente e dividido pela quantidade de respondentes, neste caso dez.

O Quadro 7 apresenta os processos e suas respectivas médias de maturidade com base nos dados preenchidos pelos respondentes.

Nome do Processo	Maturidade Média Pesquisa
POA - Planejamento, Organização e Alinhamento	
POA01 - Planejamento Estratégico da Segurança da Informação	1,2
POA02 - Política de Segurança da Informação	1,6
POA03 - Organização Interna	1,3
POA04 - Organização com as Partes Externas	1,3
POA05 - Gestão de Risco	1,3
ORG - Segurança Organizacional	
ORG01 - Responsabilidade pelos Ativos	1,2
ORG02 - Classificação da Informação	1,5
ORG03 - Segurança em Recursos Humanos	1,6
ORG04 - Procedimentos e Responsabilidades Operacionais	1,8
ORG05 - Troca de Informações	1,6
ORG06 - Requisitos de Negócio para Controle de Acesso	2,1
ORG07 - Responsabilidade dos Usuários	2,6
ORG08 - Requisitos de Segurança de Sistemas de Informação	1,8
FIS - Segurança Física	
FIS01 - Áreas Seguras	2,1
FIS02 - Segurança em Equipamentos	2,1
TEC - Segurança Técnica	
TEC01 - Gerenciamento de Serviços de Terceiros	2,1
TEC02 - Planejamento e Aceitação dos Sistemas	2,1
TEC03 - Proteção contra Códigos Maliciosos e Códigos Móveis	1,4
TEC04 - Cópias de Segurança	2,7
TEC05 - Gerenciamento da Segurança em Redes	2,7

TEC06 - Manuseio de Mídias	1,8
TEC07 - Serviços de Comércio Eletrônico	1,6
TEC08 - Gerenciamento de Acesso do Usuário	2,8
TEC09 - Controle de Acesso a Rede	1,9
TEC10 - Controle de Acesso ao Sistema Operacional	1,7
TEC11 - Controle de Acesso a aplicação e a Informação	1,8
TEC12 - Computação Movel e Trabalho Remoto	1,4
TEC13 - Processamento Correto nas Aplicações	1,9
TEC14 - Controles Criptográficos	2,8
TEC15 - Segurança dos Arquivos do Sistema	1,6
TEC16 - Segurança em Processos de Desenvolvimento e de Suporte	2,0
TEC17 - Gestão de Vulnerabilidades Técnicas	1,3
GES - Gestão da Segurança	
GES01 - Notificação de Fragilidades e Eventos de Segurança da Informação	1,1
GES02 - Gestão de Incidentes de Segurança da Informação e Melhorias	1,9
GES03 - Monitoramento de Atividades	2,7
GES04 - Aspectos da Gestão de Continuidade de Negócios em Segurança da Informação	2,4
GES05 - Conformidade com Requisitos Legais	1,5
GES06 - Conformidade com normas, políticas de Segurança da Informação e Conformidade Técnica	1,1
GES07 - Considerações quanto a Auditoria de Sistemas de Informação	2,6

Quadro 7 – Resultados com a média da maturidade dos processos.
Fonte: O Autor.

Para facilitar a visualização dos resultados do Quadro 7, o próprio sistema de informações gerou um gráfico do tipo radar, que pode ser visualizado na Figura 8.

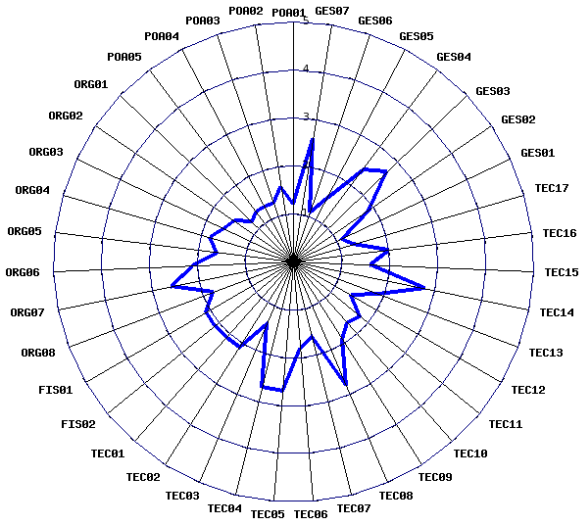

Figura 8 - Gráfico radar representando a média da maturidade dos processos avaliados na pesquisa.
Fonte: O Autor.

Analisando os resultados é possível concluir que as organizações avaliadas possuem variação na maturidade dos processos de segurança da informação, uma vez que existe pico de maturidade no valor de 2,8 contra valor mínimo de 1,1. Esta variação leva a entender que alguns processos são mais bem trabalhados do que outros sob a ótica da norma ABNT NBR ISO/IEC 27002:2005. Pode-se concluir que as organizações participantes tratam o mesmo processo de maneiras diferentes entre si. Por se tratar de processo, o principal motivo esta variação é diferença da cultura da gestão de processos nas organizações.

Observamos que à página 17 deste trabalho sugere-se que as escalas não devem possuir granularidade de, por exemplo, 1,15. Não há conflito entre tal sugestão e o resultado aqui apresentado, pois não se trata da escala, mas sim do resultado médio, o qual indica-nos um direcionamento: as organizações tendem ou estão mais próximas do nível mais baixo de maturidade.

5.2 Processos com maior e menor média de maturidade

Os oito processos que mais se destacam nesta análise da média geral são: TEC08 - Gerenciamento de Acesso do Usuário, com média 2,8; TEC14 - Controles Criptográficos, com média 2,8; TEC04 - Cópias de Segurança, com média 2,7; TEC05 - Gerenciamento da Segurança em Redes, com média 2,7; GES03 - Monitoramento de Atividades, com média 2,7; GES07 - Considerações quanto a Auditoria de Sistemas de Informação, com média 2,6; ORG07 - Responsabilidade dos Usuários, com média 2,6; GES04 - Aspectos da Gestão de Continuidade de Negócios em Segurança da Informação, com média 2,4.

Observando estes processos e seus objetivos pode-se concluir que o assunto que há mais tempo a tecnologia da informação aborda nas boas práticas são os mais evoluídos: backup está relacionado ao processo TEC04; segurança de redes está relacionado ao processo TEC05; controle do usuário está relacionado ao processo TEC08; criptografia está relacionada ao processo TEC14. Lembrando que os processos do domínio TEC têm como característica serem aplicados aos ambientes de Tecnologia da Informação, como colocado no item 4.1.2.

Por outro lado, quatro processos se destacaram por possuir a menor média geral: GES01 - Notificação de Fragilidades e Eventos de Segurança da Informação, com média 1,1; GES06 - Conformidade com normas, políticas de Segurança da Informação e Conformidade Técnica, com média 1,1; POA01 - Planejamento Estratégico da Segurança da Informação, com média 1,2; ORG01 - Responsabilidade pelos Ativos, com média 1,2.

Observando estes processos e seus objetivos pode-se concluir que o assunto é mais recente na tecnologia da informação, abordando principalmente o tema gestão e conformidade: conformidade está relacionada ao processo GES06; planejamento está relacionado ao processo POA01; gestão de eventos está relacionada aos processos GES01. Lembrando que os processos do domínio GES possuem como objetivo a gestão da segurança da informação, como colocado no item 4.1.2.

5.3 Domínios que apresentaram a maior e menor média de maturidade

A média de um domínio foi calculada somando a média de todos os processos de domínio e dividindo pela quantidade de processos do mesmo e fornece valores meramente indicativos da posição geral.

Um domínio apresentou a maior média, no valor de 2,1: FIS - Segurança Física, seguido pelo domínio TEC - Segurança Técnica com a média 1,97. Analisando os processos que compõe estes domínios, chegamos à conclusão que são os domínios onde estão os assuntos que há mais tempo a tecnologia da informação aborda nas boas práticas e que são os mais evoluídos. A Figura 9 apresenta o ranking dos domínios e suas médias.

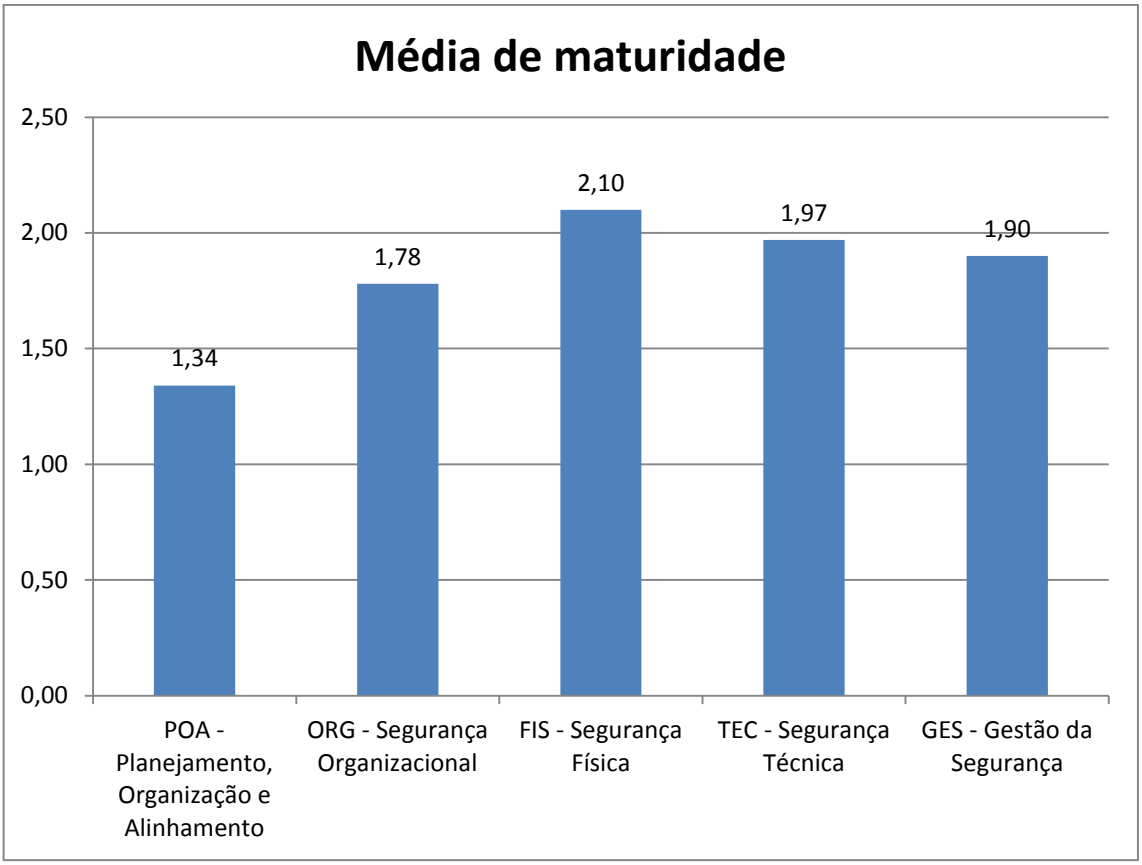

Figura 9 - Média de maturidade por domínio.
Fonte: O Autor.

Com base na Figura 9 podemos entender que o domínio com menor média é o POA - Planejamento, Organização e Alinhamento, com média de 1,34. Isso reforça a conclusão que os assuntos relacionados à gestão e planejamento são os menos evoluídos no que tange a segurança da informação. Isto é ruim por resultar em que a segurança deixa de ser proativa e passa a ser reativa.

5.4 Resultados individuais de cada respondente

Todos os respondentes tiveram a oportunidade de visualizar seus resultados comparados com a média aritmética da pesquisa. Como exemplo, a Figura 10 representa o gráfico de maturidade do respondente 1.

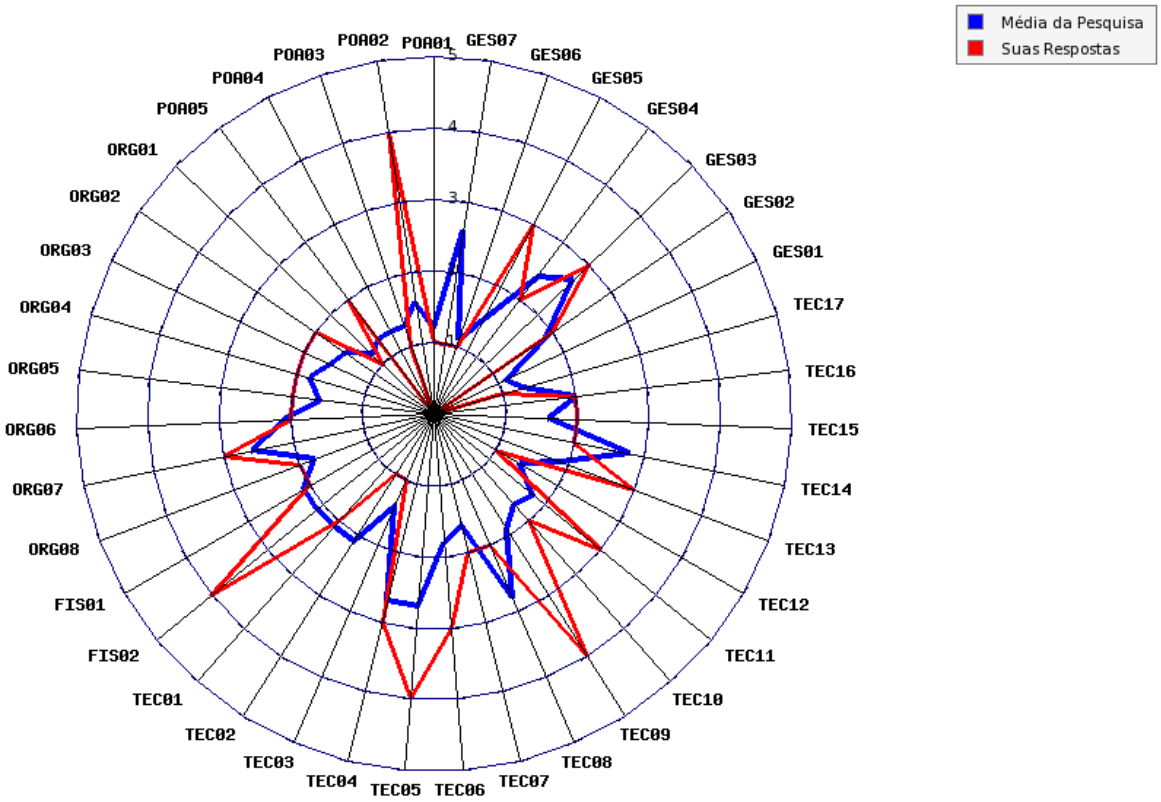

Figura 10 - Resultado completo da análise de maturidade do respondente 1.
Fonte: O Autor.

Analisando individualmente os resultados e comparando entre os respondentes, é possível concluir que o tema segurança da informação já está sendo tratado de maneira mais eficiente em algumas organizações, mas ainda demonstra que tem muito a evoluir.

Os respondentes que mais chamaram a atenção, devido os resultados de maturidade obtidos, podem ser visualizados na Figura 11, que apresenta os resultados destes respondentes para os três maiores níveis de maturidade.

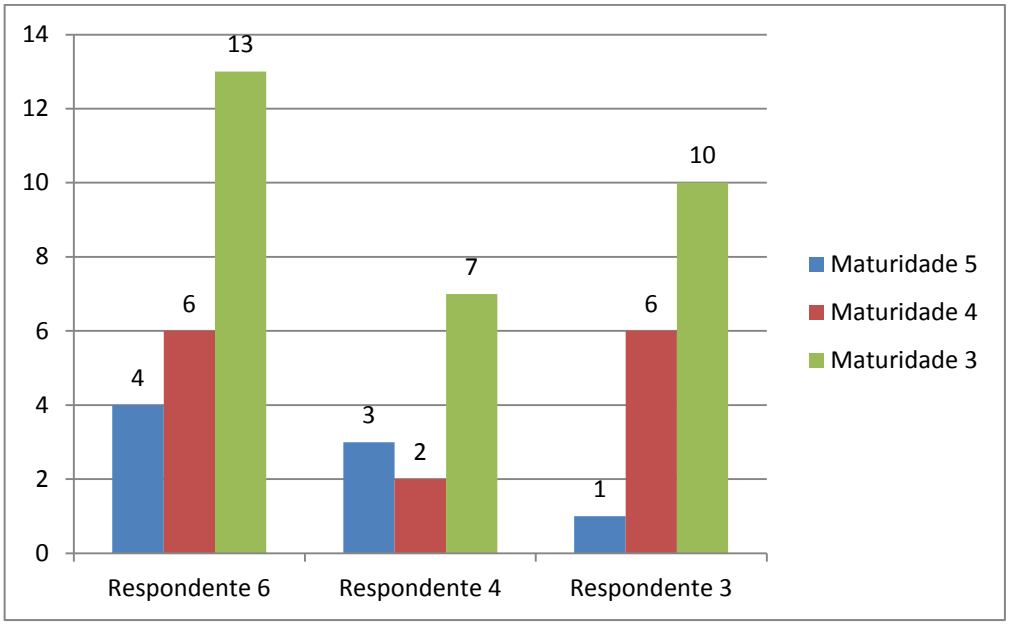

Figura 11 - Número de respostas por nível de maturidade por respondente.
Fonte: O Autor.

Analisando o respondente número 6 e consolidando os resultados, ele possui vinte e três processos com maturidade no mínimo no nível 3, o que equivale a cinquenta e nove por cento (59%) de todos os processos definidos.

5.5 Considerações finais

Este trabalho atingiu seu objetivo de desenvolver uma proposta de uma estrutura de análise de maturidade dos processos de segurança da informação com base na norma ABNT NBR ISO/IEC 27002:2005. Esta proposta pode oferecer a uma organização uma comparação de suas ações e iniciativas de segurança da informação com os processos padrões estabelecidos pela norma ABNT NBR ISO/IEC 27002:2005.

Para se chegar ao objetivo foi proposta uma estrutura de processos que represente os objetivos de controle estabelecidos na norma ABNT NBR ISO/IEC 27002:2005, que foi desenvolvida a partir do entendimento e identificação dos objetivos de controle da norma.

A partir da proposta dos processos e com o apoio do modelo genérico de maturidade do CMMI, foi desenvolvido um modelo de análise de maturidade para os trinta e nove (39) processos que contemplem os objetivos de controle da norma ABNT NBR ISO/IEC 27002:2005.

Para avaliar a maturidade com base no modelo de maturidade proposto, foi elaborado um questionário para cada processo, que, apoiado por uma ferramenta computacional, formam a proposta de análise de maturidade deste trabalho. O questionário foi aplicado para dez (10) organizações da região de Curitiba-PR que possuem no mínimo mil usuários internos de tecnologia da informação.

Basicamente este horizonte de aplicação limitado deve-se: ao tempo disponível dentro das limitações de um mestrado; a não existência de organizações de porte disponíveis e que, ao mesmo tempo, concordem em “abrir” suas condições de segurança da informação, tema sensível e estratégico.

É importante ressaltar o caráter inédito da pesquisa, até o momento e no horizonte consultado, uma vez que a proposta de uma estrutura de processos de segurança da informação com base na norma, seu respectivo modelo de maturidade e seu questionário são inovadores e foram pela primeira vez propostos.

A análise dos resultados apresentou a diferença na abordagem do tema segurança da informação entre as organizações, uma vez que foram identificados níveis de maturidade diferentes para os mesmos processos avaliados nas organizações participantes. Isso se deve principalmente por dois motivos: a) a cultura de gestão de processos que cada organização possui; b) a evolução do tema segurança da informação em cada organização.

Estes resultados também colaboram com a visão que a segurança da informação ainda é um tema tratado sob a responsabilidade da área de tecnologia da informação das organizações. Isso se dá devido à influência que o tema segurança da informação tem em relação à área de tecnologia da informação. A segurança da informação surgiu como uma necessidade de proteção da informação digital (suportada pela tecnologia da informação) e aos poucos está sendo estendida para todo o domínio da organização.

Por outro lado, os resultados mostraram que as questões de planejamento e gestão ainda são pontos fracos da segurança da informação, refletindo a carência destes temas na área de tecnologia da informação.

A estratégia do uso da norma ABNT NBR ISO/IEC 27002:2005 e a metodologia adotada na construção da proposta de maturidade se mostraram satisfatórios na identificação de pontos de melhoria nos processos de segurança da informação.

O uso da ferramenta computacional desenvolvida apoiou de maneira rápida a consolidação dos resultados e se mostrou eficiente para aplicação da pesquisa, uma vez que todos os respondentes concluíram o preenchimento da pesquisa. Ao mesmo tempo possibilitou *feedback* imediato aos respondentes

Por fim, a utilização do modelo de maturidade genérico do CMMI foi plenamente seguida no desenvolvimento dos modelos de maturidade dos processos, confirmando a sua flexibilidade de uso. Esta flexibilidade pode ser rapidamente constatada por meio das Figuras 11-14, no apêndice A.

5.5.1 Trabalhos futuros

Com a finalidade de contribuir para um maior detalhamento do tema abordado, seguem algumas sugestões para o desenvolvimento de trabalhos futuros:

a) Elaboração de uma estrutura de controle de processos de segurança da informação mais detalhada, com o desenvolvimento de modelos de gestão, indicadores de desempenho e resultados, alocação de responsabilidade e fluxos de atividades;
b) Aplicação dos modelos de maturidade em universos maiores e representativos de áreas de interesse geral, como administração pública direta;
c) Aplicação da metodologia de desenvolvimento de modelo de maturidade em outras normas da série ISO, com o objetivo de propor avaliações de maturidade em escopos ainda não previstos, mas regidos por normas internacionais.

REFERÊNCIAS

ANDRADE, F. F. de. **O Método de Melhorias PDCA**. Dissertação (Mestrado em Engenharia) – Universidade de São Paulo, São Paulo, 2003.

ANTUNES JÚNIOR, J. A. V. **Os paradigmas na engenharia de produção**. COPPE/UFRJ, 2006.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT**. Coletânea de normas de sistemas da qualidade**. Rio de Janeiro. ABNT, 2001.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT**. ABNT NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

BAARS, H.; HINTZBERGEN, K.; HINTZBERGEN, J.; SMULDERS, A.. ***The Basis of Information Security – A Pratical Handbook***. Newton Translations, the Netherlands, 2009.

BERNARDES, M. C.; MOREIRA, E. dos S. **Um modelo para a inclusão da governança da segurança da informação no escopo da governança organizacional**. 7° Simpósio Segurança em Informática, 2005. Disponível em <ftp://www.linorg.cirp.usp.br/pub1/SSI/SSI/SSI2005/artigos/14275.pdf>. Acesso em: 03/01/2012.

BRITTO, T. D. E. - **Levantamento e diagnóstico de maturidade da governança da segurança de informação na administração direta federal brasileira**. Dissertação (Mestrado) - Universidade católica de Brasília, 2011.

BSI - British Standards Institution. ***Information Security ISO/IEC 27001***. Disponível em <http://www.bsigroup.com>. Acesso em: 10/07/2010.

BYTHEWAY, A. ***IMBOK - Information Management Body of Knowledge***. Ed. 2011. University of the Western Cape, and Cape Peninsula University of Techology, 2011.

CANONGIA, C.; MANDARINO JUNIOR, R. **Segurança cibernética: o desafio da nova Sociedade da Informação**. Revista Parcerias Estratégicas, volume 14, edição n°29. Ministério da Ciência e Tecnologia, 2009.

CAROSIA, J. **Levantamento da Qualidade do Processo de Software com Foco em Pequenas Organizações**. Dissertação (Mestrado). Instituto Nacional de Pesquisas Espaciais, 2004.

CORRÊA, P. M. **Um estudo sobre a implantação da governança de TI com base em modelos de maturidade**. Dissertação (Mestrado). Centro Estadual de Educação Tecnológica Paula Souza, 2006.

FERNANDES, A. A.; ABREU, V. F. de. **Implantando a Governança de TI: Da estratégia a Gestão de processos e serviços**. 2a edição - Rio de Janeiro:Brasport, 2008.

GSI - Gabinete de Segurança Institucional da Presidência da República do, 2010. Disponível em <http://dsic.planalto.gov.br/quem-somos>. Acesso em: 08/07/2010.

ITGI - Information Technology Governance Institute. **COBIT 4.1**, Rolling Meadows, 2008.

ITSMF – ***Information Technology Service Management Forum International – ITIL*.** Disponível em <http://www.itsmfi.org>. Acesso em: 25/06/2010.

JOHNSON, L.; PINTO, J. S. de P. – **Proposta de um Programa de Segurança da Informação para as Autarquias Federais.** Trabalho apresentado no III Congresso Tecnológico InfoBrasil. Fortaleza, 2010.

MARCIANO, J. L. P. **Segurança da Informação - uma abordagem social**. Dissertação (Mestrado). Universidade de Brasília, 2006.

MASSOCO, D. B. **Uso da metodologia Árvore de Causas na Investigação de Acidente Rural**. Dissertação (Mestrado). Universidade Federal de Santa Maria, 2008.

MOURA, L. R.. **Qualidade simplesmente total: uma abordagem simples e prática da gestão da qualidade**. Rio de Janeiro: Qualitymark Ed., 1997.

NCC - ***National Computing Center***. Disponível em <http://www.ncc.co.uk>. Acesso em: 18/12/2011.

OCDE - Organização para a Cooperação e o Desenvolvimento Econômico. **Members and partners**. Disponível em <http://www.oecd.org>. Acesso em: 05/01/2012.

PACAK, A. de M.; BRANDÃO, C. R. dos R.; GUALDESSI, J. C.;DA SILVA, J. M. **Proposta de uma estrutura de controle para aderência a norma ABNT NBR 16001:2004**. Trabalho de conclusão de curso (Graduação). Faculdade Educacional Araucária, 2010.

PMI - Project Management Institute. **PMBOK 4.0**. Disponível em <http://www.pmi.org>. Acesso em: 01/07/2010.

RNP - RNP na Mídia – **Edição Eletrônica da Rede Nacional de Ensino e Pesquisa, 2007**. Disponível em <http://www.rnp.br/noticias/imprensa/2007/not-imp-070517b.html>. Acesso em 08/07/2010.

SANTOS, A. R. dos. **Metodologia Científica a construção do conhecimento**. 2. ed. - Rio de Janeiro: DP&A editora, 1999.

SANTOS, R. P. C.. **As tarefas para gestão de processos**. Tese de Doutorado em Engenharia de Produção. 454p. COPPE/UFPR, 2007.

SCHIFFMAN, L. & KANUK, L. **Comportamento do consumidor**. LTC Editora. 6a ed. 2000.

SILVA, D. F. A. e. **Modelo de Maturidade de Processos de Gestão Acadêmica em Instituições Privadas de Ensino Superior**. Dissertação (Mestrado). Centro Estadual de Educação Tecnológica Paula Souza, 2009.

SIQUEIRA, J. **O Modelo de Maturidade de Processos: Como Maximizar o Retorno dos Investimentos em Melhoria da Qualidade e Produtividade**. Disponível em: <http://www.ibqn.com.br/htm_artigos_links/Jairo_Siqueira_Artigo_Modelo de Maturidade.pdf>. Acesso em: 20/07/2010.

TESSARI, R. **Gestão de processos de negócios: um estudo de caso da BPM em uma empresa do setor moveleiro**. Dissertação (Mestrado). Universidade de Caxias do Sul, 2008.

TCU – Tribunal de Contas da União. **Relatório de levantamento. Avaliação da Governança de Tecnologia da Informação na Administração Pública Federal. Constatação de Precariedades e Oportunidades de Melhoria. Determinações, Recomendações e Comunicações**. Brasília, TCU, 2010.

WINKELMANN, D. L. B. **ISO/IEC 27002 – Avaliando o código de boas práticas em segurança da informação e propostas de ferramentas e soluções**. Trabalho de conclusão de curso (Graduação). Escola Superior de Estudos Empresariais e Informática, 2008.

APÊNDICE A – CÓPIAS DE TELAS DA FERRAMENTA COMPUTACIONAL DESENVOLVIDA

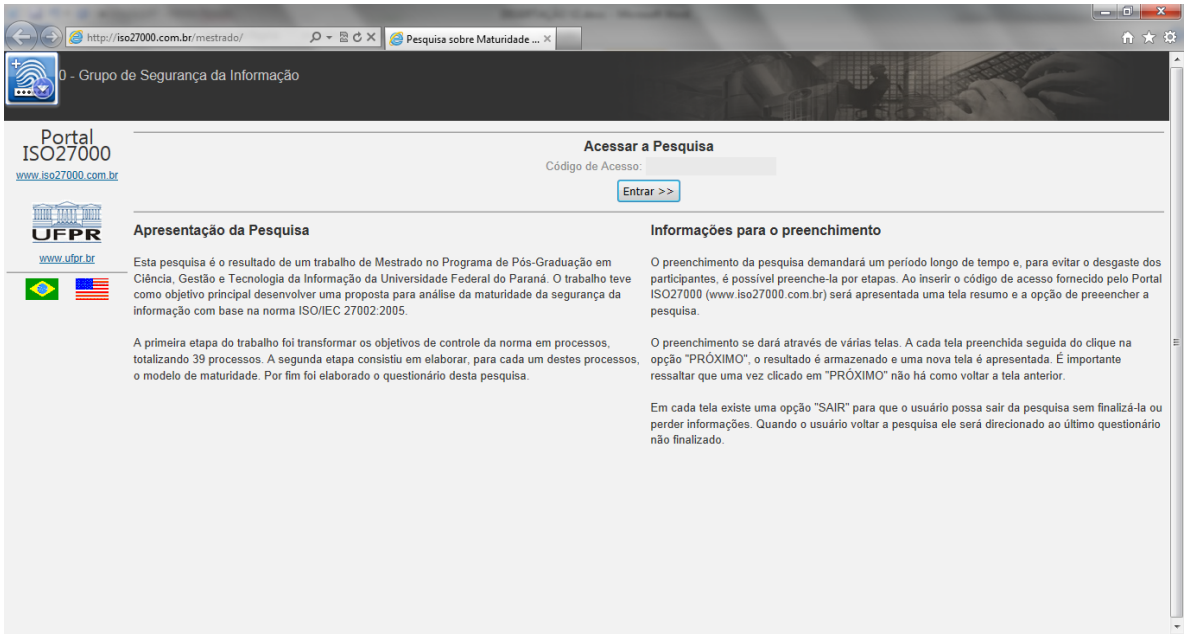

Figura 12: Tela principal do sistema.
Fonte: O Autor.

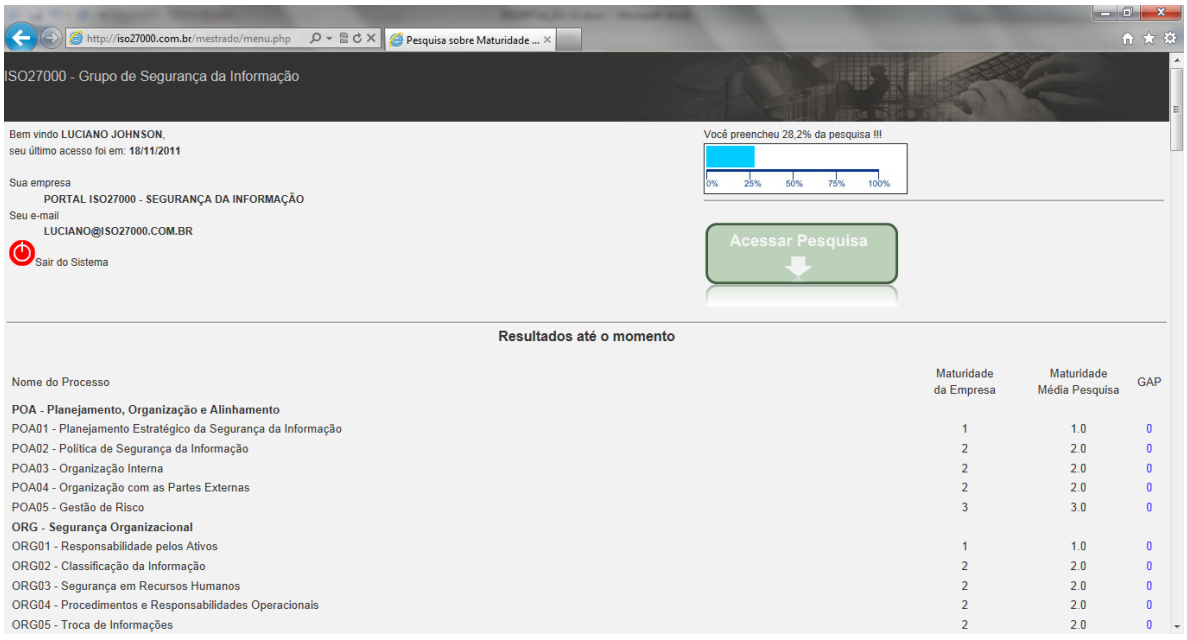

Figura 13: Tela principal do usuário do sistema.
Fonte: O Autor.

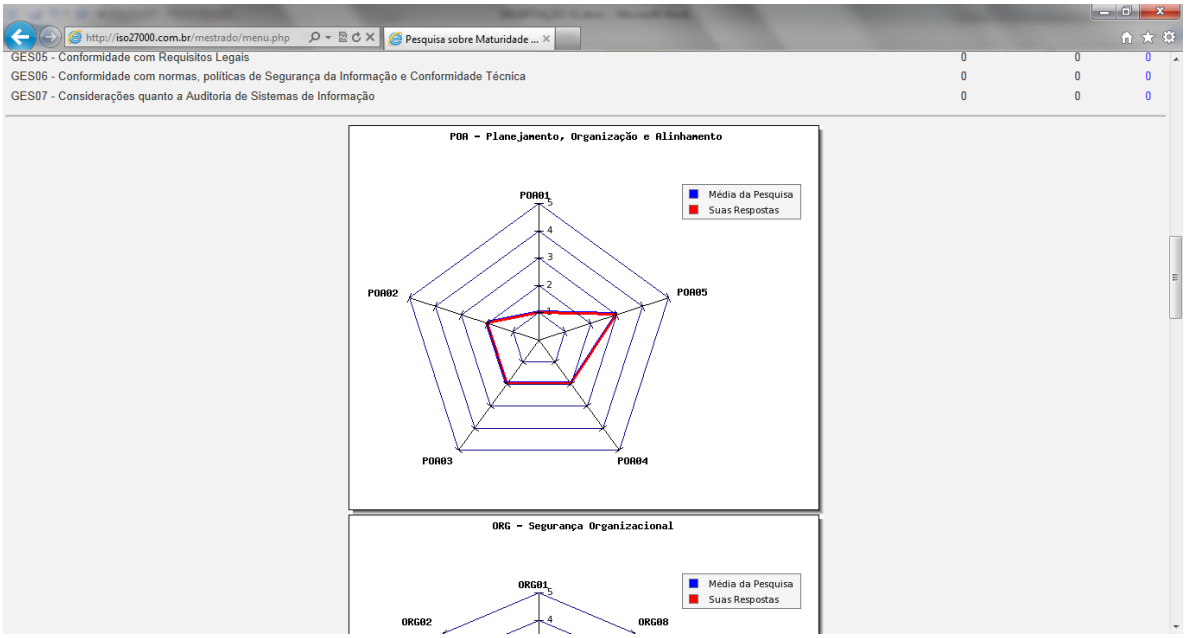

Figura 14: Tela de resultados on-line do sistema.
Fonte: O Autor.

Figura 15: Tela do questionário do sistema.
Fonte: O Autor.

APÊNDICE B – DESCRIÇÃO DOS PROCESSOS DE CONTROLE PARA ANÁLISE DA MATURIDADE

DESCRIÇÃO DO PROCESSO

POA01 – Planejamento Estratégico da Segurança da Informação

O planejamento estratégico da segurança da informação é necessário para gerenciar todos os recursos de segurança da informação em alinhamento com as prioridades e estratégias organizacionais e de negócio. A segurança da informação, assim como e as partes interessadas pelas operações de negócio da organização são responsáveis por assegurar que as próprias operações de negócio possuem os níveis requeridos de segurança da informação através de um programa de segurança da informação. O plano estratégico deve aprimorar o entendimento das partes envolvidas no que diz respeito a oportunidades e limitações que a segurança da informação possa impor, assim como avaliar o desempenho das atuais soluções de segurança e esclarecer o nível de investimento requerido para tal. A estratégia e as prioridades de negócio devem ser refletidas no programa de segurança da informação e executadas por meio de planos táticos de segurança que estabeleçam objetivos concisos, tarefas e que representem com clareza os resultados desejados.

OBJETIVOS DE CONTROLE

POA01.1 – Gerenciamento de valor da segurança da informação

Trabalhar sob as diretrizes da operação de negócio para assegurar que o programa de segurança da informação e seus investimentos estejam devidamente embasados em sólidos estudos de caso de negócio. Reconhecer que há investimentos obrigatórios, sustentáveis e discricionários que diferem em complexidade e grau de liberdade na alocação de fundos. Os processos de segurança da informação devem prover a entrega eficaz e eficiente de soluções e estruturas, assim como fornecer advertência de qualquer desvio dos planos, incluindo custo, cronograma ou funcionalidade, que possa afetar os resultados esperados dos programas. As ações de segurança da informação devem ser executadas em conformidade com acordos de níveis de serviço (*service level agreeement*, SLA) equilibrados e controláveis. A responsabilidade pelo alcance dos benefícios e o controle dos custos deve ser claramente atribuída e monitorada. Estabelecer avaliação adequada, transparente, repetível e comparável de estudos de caso de negócio, incluindo valor financeiro, o risco de não fornecer uma capacidade e o risco de não atingir os benefícios esperados.

POA01.2 – Alinhamento entre o negócio e a segurança da informação

Estabelecer processos de educação bidirecional e envolvimento recíproco no planejamento estratégico para atingir o alinhamento e a integração de negócios e a segurança da informação. Mediar os imperativos de negócios e de segurança da informação para que as prioridades sejam mutuamente aceitas.

POA01.3 – Avaliação da capacidade e desempenho correntes

Avaliar a capacidade e o desempenho atuais das entregas de soluções e serviços de segurança da informação para estabelecer um modelo com o qual os requisitos futuros podem ser comparados. Definir o desempenho em termos da contribuição da segurança da informação com os objetivos de negócio, funcionalidades, estabilidade, complexidade, custos, pontos fortes e fragilidades.

POA01.4 – Plano estratégico da segurança da informação

Criar um plano estratégico que defina, em cooperação com as partes interessadas relevantes, como a segurança da informação contribuirá com os objetivos estratégicos da organização e suas metas, e quais os custos e riscos relacionados. Esse plano estratégico deve contemplar como a segurança da informação aplicará os programas de investimentos e como dará sustentação à entrega operacional de serviços e soluções de segurança. O plano deve definir como os objetivos serão atingidos e medidos e deve ser formalmente liberado para implementação pelas partes interessadas. O plano estratégico da

segurança da informação deve contemplar o orçamento operacional e de investimento, as fontes de recursos financeiros, a estratégia de fornecimento, a estratégia de aquisição e requisitos legais e regulamentares. O plano estratégico deve ser suficientemente detalhado para possibilitar a definição do programa de segurança da informação.

POA01.5 – Programa de segurança da informação
Criar um programa de segurança da informação derivado do plano estratégico da segurança da informação. Esse programa deve descrever quais são as iniciativas de segurança requeridas, quais os recursos necessários e como o uso de recursos e os benefícios alcançados serão monitorados e administrados. O programa de segurança da informação deve ser suficientemente detalhado de forma a permitir o desenvolvimento de planos de projetos.

POA01.6 – Gerenciamento do programa de segurança da informação
Gerenciar ativamente com as áreas de negócio o programa de investimentos de segurança da informação necessários para atingir os objetivos estratégicos específicos de negócio, através de identificação, definição, avaliação, priorização, seleção, início, gerenciamento e controle de programas. Isso inclui esclarecer os resultados de negócio desejados, assegurar que os objetivos do programa sustentem o alcance dos resultados, entender o escopo completo do esforço necessário para atingir os resultados, atribuir responsabilidades com medidas de suporte, definir projetos dentro do programa, alocar recursos e fundos, delegar autoridade e atribuir responsabilidades pelos projetos no lançamento do programa.

MODELO DE MATURIDADE

POA01 – Planejamento Estratégico da Segurança da Informação

0 Não existente quando
O plano estratégico da segurança da informação não existe. A Direção não está conscientizada de que o planejamento estratégico da segurança da informação é necessário para sustentar as metas de negócio.

1 Inicial/*Ad Hoc* quando
A necessidade de um planejamento estratégico da segurança da informação é conhecida pela Direção da organização. O planejamento da segurança da informação é realizado caso a caso, em resposta a um requisito específico de negócio. O planejamento estratégico da segurança da informação é ocasionalmente discutido nas reuniões da Direção. O alinhamento de requisitos de negócio, aplicações e tecnologia ocorre de forma reativa ao invés de seguir uma estratégia corporativa. A posição estratégica de risco é identificada informalmente projeto a projeto.

2 Repetível mas intuitivo quando
O planejamento estratégico da segurança da informação é compartilhado com a Direção do Negócio conforme a necessidade. A atualização dos planos de segurança acontece em resposta aos pedidos da Direção. As decisões estratégicas são tomadas projeto a projeto, sem consistência com uma estratégia corporativa. Os riscos e benefícios do usuário nas principais decisões estratégicas são determinados de forma intuitiva.

3 Definido quando
Uma política define quando e como realizar um planejamento estratégico da segurança da informação. O planejamento estratégico da segurança da informação segue uma abordagem estruturada, que é documentada e conhecida por todo o pessoal envolvido. O processo do planejamento da segurança da informação é razoavelmente discutido e assegura que um planejamento adequado seja realizado. Entretanto, a implementação do processo fica a critério de cada Direção e não há procedimentos para examinar o processo. A estratégia geral da segurança da informação inclui uma definição consistente dos riscos que a organização aceita correr por ser inovadora ou por seguir tendências. As estratégias de recursos financeiros, técnicos e humanos influenciam cada vez mais na aquisição de novos produtos e tecnologias. O planejamento estratégico da segurança da informação é discutido nas reuniões de gerenciamento do negócio.

4 Gerenciado e Mensurável quando
O planejamento estratégico da segurança da informação é uma prática padrão cujas exceções são detectadas pela Direção. O planejamento estratégico da segurança da informação é uma função da Direção com nível sênior de responsabilidade. A Direção é capaz de monitorar o processo de planejamento estratégico da segurança da informação, tomar decisões baseadas nesse processo e medir sua efetividade. Os planejamentos da segurança da informação, de curto e longo prazo são cascateados de cima para baixo na organização, com atualizações quando necessário. A estratégia da segurança da informação e a estratégia global da organização estão se tornando gradativamente mais coordenadas por abordar processos de negócio, capacidades de valor agregado e alavancar o uso de aplicativos e tecnologias na reengenharia dos processos de negócios. Há um processo bem definido para determinar o uso dos recursos internos e externos no desenvolvimento de soluções que suportem o negócio e sua perenidade.

5 Otimizado quando
O planejamento estratégico da segurança da informação é um processo documentado e dinâmico,

sempre considerado no estabelecimento dos objetivos de negócio, e resulta em valor de negócio identificável através dos investimentos em segurança. As considerações de risco e o valor agregado são continuamente atualizados no processo de planejamento estratégico da segurança da informação. Planos realísticos de segurança de longo prazo são desenvolvidos e constantemente atualizados para refletir mudanças na tecnologia e no desenvolvimento relativos ao negócio. Comparações com normas confiáveis e bem conhecidas do mercado são realizadas e integradas ao processo de formulação de estratégias (*benchmarking*). O planejamento estratégico inclui uma análise de como as novas tecnologias podem criar novas capacidades de negócio e melhorar a vantagem competitiva da organização, sua continuidade e resiliência.

QUESTIONÁRIO DE MATURIDADE

POA01 – Planejamento Estratégico da Segurança da Informação

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
O planejamento da segurança da informação é realizado em resposta a um requisito específico de negócio.		X		
O planejamento estratégico da segurança da informação é discutido nas reuniões da Direção.	X			
O alinhamento de requisitos de negócio, aplicações e tecnologia ocorre de forma reativa..		X		
A segurança da informação se confunde com a segurança de TI.		X		
Maturidade Nível 2				
O planejamento estratégico da segurança da informação é compartilhado com a Direção do Negócio conforme a necessidade.			X	
As decisões estratégicas são tomadas projeto a projeto, sem consistência com uma estratégia corporativa.			X	
Os riscos e benefícios nas principais decisões estratégicas são determinados de forma intuitiva		X		
Maturidade Nível 3				
Uma política define quando e como realizar um planejamento estratégico da segurança da informação.				X
O planejamento estratégico da segurança da informação segue uma abordagem estruturada, documentada e conhecida pelos envolvidos.				X
As estratégias de recursos financeiros, técnicos e humanos influenciam na aquisição de novos produtos e tecnologias.			X	
O planejamento estratégico da segurança da informação é discutido nas reuniões de gerenciamento do negócio.			X	
Maturidade Nível 4				
O planejamento estratégico da segurança da informação é uma prática padrão cujas exceções são detectadas pela Direção.				X
O planejamento estratégico da segurança da informação é uma função da Direção com nível sênior de responsabilidade			X	
A estratégia da segurança da informação e a estratégia global da organização estão gradativamente mais coordenadas.			X	
Há um processo bem definido para determinar o uso dos recursos internos e externos no desenvolvimento de soluções que suportem o negócio.				X

Maturidade Nível 5				
O planejamento estratégico da segurança da informação é um processo documentado e dinâmico, sempre considerado no estabelecimento dos objetivos de negócio.				X
As considerações de risco e o valor agregado são continuamente atualizados no processo de planejamento estratégico da segurança da informação.				X
O planejamento estratégico inclui uma análise de como as novas tecnologias podem criar novas capacidades de negócio e melhorar a vantagem competitiva da organização, sua continuidade e resiliência.			X	
Existem métricas para avaliar o planejamento e seus resultados.				X

DESCRIÇÃO DO PROCESSO

POA02 – Política de Segurança da Informação

Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentações pertinentes. Convém que a direção estabeleça uma clara orientação da política, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

OBJETIVOS DE CONTROLE

POA02.1 – Documento da política de segurança da informação

Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes**.**

POA02.2 – Análise crítica da política de segurança da informação

Convém que a política de segurança da informação seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia**.**

MODELO DE MATURIDADE

POA02 – Política de Segurança da Informação

0 Não existente quando
A organização não possui e também não é sensibilizada em relação as políticas de segurança da informação.

1 Inicial/*Ad Hoc* quando
A organização já reconheceu que existem necessidades de segurança da informação e que a política de segurança da informação é um dos primeiros passos a ser dado. Existem algumas regras de segurança, mas que não se configuram como uma política plena e são pontualmente aplicadas.

2 Repetível mas intuitivo quando
Já existem documentos que formam um conjunto de regras de segurança da informação, mas sua aplicação ainda não é completa pela organização. Os colaboradores já possuem conhecimento sobre as questões segurança, mas ainda não é formalmente a posição da diretoria, assim como ainda não representa diretrizes.

3 Definido quando
A direção revisou e aprovou formalmente uma política de segurança da informação, composta por diretrizes claras e objetivas. Os colaboradores foram devidamente informados desta política, assim como passaram por um treinamento. Ainda não existe uma análise crítica da política de segurança da informação, assim como também ainda não existem processos de monitoramento e gerenciamento de sua aplicação.

4 Gerenciado e Mensurável quando
Existe um gerenciamento e monitoramento da aplicação da política de segurança da informação e de como os colaboradores a respeitam. Foi criada uma comissão para análise crítica da política e sua revisão é anual. São gerados indicadores relacionados a aderência da política pela organização e seus terceiros.

5 Otimizado quando
O documento da política de segurança da informação é refinado constantemente através dos feedbacks das análises críticas. A aderência a política é constantemente avaliada e desvios são rapidamente identificados, avaliados. A organização e seus terceiros já identificam a política de segurança da informação como uma ferramenta eficiente e eficaz que suporta os requisitos de negócio corporativos.

QUESTIONÁRIO DE MATURIDADE

POA02 – Política de Segurança da Informação

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem regras de acesso e uso de tecnologia, visando proteger a organização.	X			
Alguns controles de seguranças são relacionados como políticas.		X		
Maturidade Nível 2				
Existem documentos que formam um conjunto de regras de segurança da informação.		X		
Os colaboradores já possuem conhecimento sobre as questões segurança.			X	
As ações e procedimentos de seguranças possuem abrangência na organização.			X	
Maturidade Nível 3				
A direção revisou e aprovou formalmente uma política de segurança da informação, composta por diretrizes claras e objetivas.				X
Os colaboradores foram devidamente informados desta política, assim como passaram por um programa de conscientização.				X
A análise da política é reativa a pontos reportados por colaboradores.			X	
Maturidade Nível 4				
Existe um gerenciamento e monitoramento da aplicação da política de segurança da informação.				X
Existe uma comissão para análise crítica da política e sua revisão é periódica.			X	
São gerados indicadores relacionados a aderência da política pela organização e seus terceiros.			X	
Maturidade Nível 5				
A política de segurança da informação é refinada constantemente através dos feedbacks das análises críticas.				X
A aderência a política é constantemente avaliada e desvios são rapidamente identificados, avaliados e corrigidos.				X
A organização e seus terceiros já identificam a política de segurança da informação como uma ferramenta eficiente e eficaz que suporta os requisitos de negócio corporativos.			X	

DESCRIÇÃO DO PROCESSO

POA03 – Organização Interna

Gerenciar a segurança da informação dentro da organização. Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização.

OBJETIVOS DE CONTROLE

POA03.1 – Comprometimento da direção com a segurança da informação
Convém que a direção apoie ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e reconhecendo as responsabilidades pela segurança da informação.

POA03.2 – Coordenação da segurança da informação
Convém que as atividades de segurança da informação sejam coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.

POA03.3 – Atribuição de responsabilidades para a segurança da informação
Convém que todas as responsabilidades pela segurança da informação estejam claramente definidas.

POA03.4 – Processo de autorização para os recursos de processamento da informação
Convém que seja definido e implementado um processo de gestão de autorização para os novos recursos de processamento de informação.

POA03.5 – Acordos de confidencialidade
Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados e analisados criticamente, de forma regular.

POA03.6 – Contato com autoridades
Convém que contatos apropriados com autoridades pertinentes sejam mantidos.

POA03.7 – Contato com grupos especiais
Convém que sejam mantidos contatos apropriados com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais.

POA03.8 – Análise crítica independente de segurança da informação
Convém que o enfoque da organização para gerenciar a segurança da informação e sua implementação seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.

MODELO DE MATURIDADE

POA03 – Organização Interna

0 Não existente quando
A organização ainda não possui uma organização interna específica para tratar da segurança da informação, se limitando apenas ao controle da política.

1 Inicial/*Ad Hoc* quando
A direção da organização já demonstra sinais de comprometimento, participando esporadicamente de reuniões e tomadas de decisão. A segurança da informação é executada pelo departamento de tecnologia da informação da organização e ainda reflete segurança de redes. Algumas responsabilidades são atribuídas. Ainda não existem acordos de confidencialidade ou de não divulgação de informações. Os contatos com autoridades e grupos específicos são esporádicos.

2 Repetível mas intuitivo quando
A coordenação da segurança da informação organizacional ainda é executada pelo departamento de tecnologia da informação, mas com grande apoio e comprometimento da direção. Responsabilidades estão mais efetivamente atribuídas, mesmo que informalmente. Novos recursos de processamento de informações são controlados e manualmente gerenciados. Os acordos de confidencialidade são mantidos apenas para determinados colaboradores. A coordenação de segurança da informação já participa de grupos de interesse em segurança da informação com o apoio da direção. Porém, uma análise crítica independente ainda não é realizada.

3 Definido quando
A direção estabeleceu um comitê de segurança da informação composto por colaborados chaves de diversas áreas da organização com o objetivo de avaliar a segurança da informação e nortear as principais atividades de segurança a serem executadas pelas equipes responsáveis. Todos colaboradores foram informados formalmente e assinaram o documento de políticas de segurança e o acordo de confidencialidade de informações. Já existe definido um processo de tratamento de incidentes que inclui o contato com autoridades específicas e grupos de interesse.

4 Gerenciado e Mensurável quando
O comitê de segurança da informação gerencia e monitora as atividades de segurança da informação, definindo estratégias e ações corretivas e preventivas. A direção participa ativamente do comitê. A organização interna da segurança da informação já passa por uma análise crítica independente, mas ainda de maneira pontual e somente quando o comitê define como necessário.

5 Otimizado quando
A segurança da informação atingiu alto grau de organização, onde as resoluções do comitê de segurança da informação são plenamente apoiadas pela direção da organização. Todos os colaboradores reconhecem sua participação na segurança da informação e possuem responsabilidades específicas reconhecidas e formalmente atribuídas. A relação com autoridades e grupos de interesse é constante, e trás para a organização experiências e casos de negócio como exemplos. A análise crítica independente é realizada periodicamente e é fortemente incentivada pela direção.

QUESTIONÁRIO DE MATURIDADE

POA03 – Organização Interna

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
A direção da organização já demonstra sinais de comprometimento, participando de reuniões e tomadas de decisão.		X		
A segurança da informação é executada pelo departamento de TI.		X		
A segurança da informação é entendida como segurança de TI	X			
Maturidade Nível 2				
A coordenação da segurança da informação é executada pela TI.			X	
Responsabilidades estão mais efetivamente atribuídas aos colaboradores.			X	
Os acordos de confidencialidade são mantidos para os colaboradores		X		
A coordenação de segurança da informação participa de grupos de interesse em segurança da informação com o apoio da direção.		X		
Maturidade Nível 3				
Existe um comitê de segurança da informação composto por colaboradores chaves de diversas áreas da organização				X
Os colaboradores foram informados formalmente e assinaram o documento de políticas de segurança e o acordo de confidencialidade de informações				X
Existe definido um processo de tratamento de incidentes que inclui o contato com autoridades específicas e grupos de interesse			X	
Maturidade Nível 4				
O comitê de segurança da informação gerencia e monitora atividades.			X	
O comitê de segurança da informação define estratégias e ações.				X
A direção participa ativamente do comitê.				X
Maturidade Nível 5				
As resoluções do comitê de segurança da informação são apoiadas pela direção.			X	
Os colaboradores reconhecem sua participação na segurança da informação				X
A relação com autoridades e grupos de interesse é constante			X	
A análise crítica independente é realizada periodicamente e é fortemente incentivada pela direção.			X	

DESCRIÇÃO DO PROCESSO

POA04 – Organização com as Partes Externas

Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas. Convém que a segurança dos recursos de processamento da informação e da informação da organização não seja reduzida pela introdução de produtos ou serviços oriundos de partes externas.

OBJETIVOS DE CONTROLE

POA04.1 – Identificação dos riscos relacionados com partes externas

Convém que os riscos para os recursos de processamento da informação e da informação da organização oriundos de processos do negócio que envolva as partes externas sejam identificados e controles apropriados implementados antes de se conceder o acesso.

POA04.2 – Identificando a segurança da informação, quando tratando com os clientes

Convém que todos os requisitos de segurança da informação identificados sejam considerados antes de conceder aos clientes o acesso a quaisquer ativos da organização.

POA04.3 – Identificando segurança da informação nos acordos com terceiros

Convém que os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos de processamento da informação ou da informação da organização, ou acréscimo de produtos ou serviços aos recursos de processamento da informação cubram todos os requisitos de segurança da informação relevantes.

MODELO DE MATURIDADE

POA04 – Organização com as Partes Externas

0 Não existente quando
A organização ainda não se sensibilizou em organizar a segurança da informação com clientes e terceiros, sendo isso apenas uma atividade interna.

1 Inicial/*Ad Hoc* quando
Já existem algumas iniciativas em tratar a segurança da informação com partes externas, mas limitando-se a clientes. Estas iniciativas são pontuais e ocasionais. Não existe uma visão de risco na tratativa da segurança da informação.

2 Repetível mas intuitivo quando
A organização já entende melhor as necessidades de organizar a segurança da informação com partes externas, principalmente com clientes e secundariamente com os terceiros. Mas as ações ainda não são baseadas em uma avaliação de risco específica.

3 Definido quando
Foi estabelecida uma identificação de riscos no tratamento com clientes e terceiros, mas sua execução ainda é esporádica. O tratamento da segurança da informação com clientes é bem definida e aplicada. O tratamento da segurança da informação com os terceiros já se baseia nos acordos de serviço (nível de serviço e confidencialidade).

4 Gerenciado e Mensurável quando
A identificação de riscos com partes externas é regular e monitorado. As ações de segurança da informação tanto com clientes como com terceiros se tornou rotina e apresenta indicadores de aderência. Os terceiros são informados e treinados em relação às práticas de segurança da organização

5 Otimizado quando
O processo de identificação de riscos no tratamento com partes externas é gerenciado pelo comitê de segurança da informação, fornecendo análise crítica e avaliando os resultados e incidentes. Os clientes já reconhecem formalmente os procedimentos de segurança da informação, assim como os terceiros.

QUESTIONÁRIO DE MATURIDADE

POA04 – Organização com as Partes Externas

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem algumas iniciativas em tratar a segurança da informação com partes externas.		X		
Existe uma visão de risco na tratativa da segurança da informação.	X			
Maturidade Nível 2				
Existe uma organização da segurança da informação com partes externas, principalmente com clientes e secundariamente com os terceiros.		X		
Existe uma visão de risco na tratativa da segurança da informação.			X	
Maturidade Nível 3				
Existe uma identificação de riscos no tratamento com clientes e terceiros				X
O tratamento da segurança da informação com clientes é bem definido e aplicado.				X
O tratamento da segurança da informação com os terceiros se baseia nos acordos de serviço (nível de serviço e confidencialidade)			X	
Existe a comunicação e conscientização dos colaboradores sobre o tratamento de clientes e terceiros.			X	
Maturidade Nível 4				
A identificação de riscos com partes externas é regular e monitorado			X	
As ações de segurança da informação tanto com clientes como com terceiros apresenta indicadores de aderência a políticas e normas internas.				X
Os terceiros são informados e treinados em relação às práticas de segurança da organização.			X	
Maturidade Nível 5				
O processo de identificação de riscos no tratamento com partes externas é gerenciado pelo comitê de segurança da informação.			X	
Os clientes já reconhecem formalmente os procedimentos de segurança da informação, assim como os terceiros.				X
O comitê de segurança da informação faz análise crítica e avalia os resultados de controles e de incidentes			X	

DESCRIÇÃO DO PROCESSO

POA05 – Gestão de Risco

Criar e manter uma estrutura de gestão de risco. Esta estrutura documenta um nível comum e acordado de riscos de segurança da informação, estratégias de mitigação e riscos residuais. Qualquer impacto em potencial nos objetivos da organização 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.

OBJETIVOS DE CONTROLE

POA05.1 – Alinhamento da gestão de riscos de segurança da informação e de negócios
Estabelecer uma estrutura de gestão de riscos de segurança da informação alinhada com a estrutura de gestão de riscos da organização (corporação).

POA05.2 – 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.

POA05.3 – 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.

POA05.4 – 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.

POA05.5 – 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 definido.

POA05.6 – 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 direção.

MODELO DE MATURIDADE

POA05 – Gestão de Risco

0 Não existente quando
Não acontece avaliação de risco para processos e decisões de negócio. A organização não considera os impactos no negócio associados a vulnerabilidades da segurança e incertezas de projetos de desenvolvimento. Gerenciar riscos não é considerado relevante para adquirir soluções ou entregar serviços e soluções de segurança da informação.

1 Inicial/*Ad Hoc* quando
Os riscos de segurança da informação são considerados de forma ad hoc. Avaliações informais de risco de projeto são realizadas quando solicitadas em cada projeto. Riscos específicos relacionados a segurança da informação, como segurança, disponibilidade e integridade, são ocasionalmente considerados nos projetos. Os riscos de segurança da informação que afetam o dia-a-dia da operação são raramente discutidos em reuniões gerenciais. Mesmo onde os riscos são levantados, as ações para mitigá-los são inconsistentes. Está surgindo um entendimento de que os riscos de segurança da informação são importantes e devem ser considerados.

2 Repetível mas intuitivo quando
Existe uma abordagem imatura e inicial de avaliação de risco utilizada a critério de alguns colaboradores chave. A gestão de risco é superficial e geralmente aplicada somente a grandes projetos ou em resposta a problemas. O processo de mitigação de risco está começando a ser implementado onde são identificados riscos.

3 Definido quando
Uma política corporativa de gestão de risco define onde e como conduzir as avaliações de risco. A gestão de risco segue um processo definido e documentado. Há treinamento em gestão de risco disponível para todo o pessoal. Decisões de seguir o processo de gestão de risco e receber treinamento são deixadas a critério de cada indivíduo. A metodologia de avaliação de risco é convincente, robusta e assegura a identificação dos riscos–chave para o negócio. Um processo para mitigar os riscos-chave é implementado após a identificação dos riscos. As responsabilidades pela gestão de riscos estão definidas nas descrições de cargo.

4 Gerenciado e Mensurável quando
A avaliação e a gestão de risco são procedimentos padronizados. A gestão de risco de segurança da informação é uma responsabilidade do comitê de segurança da informação. O risco é avaliado e mitigado no nível de projeto e também regularmente no nível de operação de negócio. O comitê de segurança da informação é avisado das mudanças no ambiente de negócios que podem afetar consideravelmente os cenários de riscos relacionados a segurança da informação. O comitê de segurança da informação estabelece os níveis de risco que a organização irá tolerar. A área de segurança da informação desenvolveu indicadores padrão para avaliar riscos e definir taxas de riscos/retornos.

5 Otimizado quando
O gerenciamento de risco atingiu um estágio de desenvolvimento em que há um processo organizacional estruturado em vigor e bem gerenciado. A captura, a análise e o relato de dados de gestão de risco estão altamente automatizados. A gestão de risco está totalmente integrada às operações de negócio. O comitê de segurança da informação avalia continuamente as estratégias de mitigação de risco.

QUESTIONÁRIO DE MATURIDADE

POA05 – Gestão de Risco

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Os riscos de segurança da informação são considerados de forma ad hoc.		X		
Avaliações informais de risco de projeto são realizadas.	X			
Mesmo onde os riscos são levantados, as ações para mitigá-los são inconsistentes.		X		
Existe um entendimento simples sobre riscos.		X		
Maturidade Nível 2				
Existe uma abordagem simples e inicial de avaliação de risco utilizada a critério de colaboradores chave.		X		
A gestão de risco é aplicada somente a grandes projetos			X	
O processo de mitigação de risco é simples e com foco na TI.		X		
Maturidade Nível 3				
Existe uma política corporativa de gestão de risco que define onde e como conduzir as avaliações de risco.			X	
A gestão de risco segue um processo definido e documentado.				X
Há treinamento em gestão de risco disponível para todos os colaboradores.				X
As responsabilidades pela gestão de riscos estão definidas nas descrições de cargos e funções.			X	
Maturidade Nível 4				
A avaliação e a gestão de risco são procedimentos padronizados.				X
A gestão de risco de segurança da informação é uma responsabilidade do comitê de segurança da informação.			X	
O comitê de segurança da informação estabelece os níveis de risco que a organização irá tolerar.				X
A área de segurança da informação desenvolveu indicadores padrão para avaliar riscos e definir taxas de riscos/retornos.			X	
Maturidade Nível 5				
O gerenciamento de risco atingiu um estágio de desenvolvimento em que há um processo organizacional estruturado em vigor e bem gerenciado.				X
A captura, a análise e o relato de dados de gestão de risco estão altamente			X	

automatizados.				
A gestão de risco está totalmente integrada às operações de negócio				X
O comitê de segurança da informação avalia continuamente as estratégias de mitigação de risco.			X	

DESCRIÇÃO DO PROCESSO

ORG01 – Responsabilidade pelos Ativos

Alcançar e manter a proteção adequada dos ativos da organização. Convém que todos os ativos sejam inventariados e tenham um proprietário responsável. Convém que os proprietários sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles..

OBJETIVOS DE CONTROLE

ORG01.1 – Inventário dos ativos

Convém que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido.

ORG01.2 – Proprietário dos ativos

Convém que todas as informações e ativos associados com os recursos de processamento da informação tenham um proprietário designado por uma parte definida da organização.

ORG01.3 – Uso aceitável dos ativos

Convém que sejam identificadas, documentadas e implementadas regras para que sejam permitidos o uso de informações e de ativos associados aos recursos de processamento de informação.

MODELO DE MATURIDADE

ORG01 – Responsabilidade pelos Ativos

0 Não existente quando
A organização não implementou nenhum tipo de controle pelos ativos e estes são fornecidos conforme a demanda interna.

1 Inicial/*Ad Hoc* quando
A organização possui o inventário sobre alguns ativos e a seleção deste é baseada somente pelo seu valor monetário e não pelo seu valor de negócio. Apenas alguns ativos possuem proprietário, mas ainda de maneira informal.

2 Repetível mas intuitivo quando
O inventário sobre todos os ativos da organização e já possuem uma descrição de uso aceitável. Alguns proprietários já assinaram formalmente o termo de responsabilidade e propriedade, mas ainda é de maneira seletiva.

3 Definido quando
Todos os ativos possuem proprietários designados formalmente e estes receberam treinamento sobre o uso aceitável dos mesmos. Por mais que existam penalizações sobre o mau uso, elas não são aplicadas. Não existem indicadores sobre os ativos e sua aquisição e manutenção é realizada sempre sobre demanda.

4 Gerenciado e Mensurável quando
Os ativos são monitorados e gerenciados pela organização, passando por verificações agendadas. O inventário ainda não é integrado com o departamento de recursos humanos, mas todos os ativos são geridos. Os proprietários são treinados quanto ao uso aceitável e em caso de incidentes, estes são relatados e avaliados pelo comitê de segurança da informação.

5 Otimizado quando
O sistema de inventário é totalmente integrado ao sistema de recursos humanos, automatizando a alocação e remoção de propriedade. Os usuários passam por processo constante de conscientização em relação ao uso aceitável dos ativos.

QUESTIONÁRIO DE MATURIDADE

ORG01 – Responsabilidade pelos Ativos

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
A organização possui o inventário sobre os seus ativos.	X			
O controle do inventário é baseado pelo seu valor monetário e não pelo seu valor de negócio.		X		
Os ativos possuem proprietário, mas ainda de maneira informal.		X		
Maturidade Nível 2				
A organização possui o inventário sobre os seus ativos.				X
Existe uma descrição de uso aceitável dos ativos.		X		
Os proprietários dos ativos assinaram formalmente o termo de responsabilidade e propriedade			X	
Maturidade Nível 3				
Os ativos possuem proprietários designados formalmente e estes receberam treinamento sobre o uso aceitável dos mesmos.			X	
A aquisição e manutenção dos ativos é realizada sobre demanda				X
O processo de controle dos ativos é formalmente comunicado a todos os colaboradores				X
Maturidade Nível 4				
Os ativos são monitorados e gerenciados, passando por verificações agendadas.			X	
Em caso de incidentes com os ativos, estes são relatados e avaliados pelo comitê de segurança da informação.				X
O inventário é integrado com o departamento de recursos humanos.		X		
Maturidade Nível 5				
O sistema de inventário é totalmente integrado ao sistema de recursos humanos, automatizando a alocação e remoção de propriedade.				X
Os usuários passam por processo constante de conscientização em relação ao uso aceitável dos ativos.				X
Existem indicadores periodicamente analisados pela alta gerência.			X	

DESCRIÇÃO DO PROCESSO

ORG02 – Classificação da Informação

Assegurar que a informação receba um nível adequado de proteção. Convém que a informação seja classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação.

OBJETIVOS DE CONTROLE

ORG02.1 – Recomendações para classificação

Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização**.**

ORG02.2 – Rótulos e tratamento da informação

Convém que um conjunto apropriado de procedimentos para rotulação e tratamento da informação seja definido e implementado de acordo com o esquema de classificação adotado pela organização**.**

MODELO DE MATURIDADE

ORG02 – Classificação da Informação

0 Não existente quando
A organização não possui nenhum tipo de classificação e identificação da informação. A informação tem acesso irrestrito dentro da organização.

1 Inicial/*Ad Hoc* quando
Algumas informações já possuem um tratamento diferenciado baseado na hierarquia funcional dos colaboradores, mas isso não se estende a todas as informações. Os critérios de acesso são dúbios e poucas vezes analisados.

2 Repetível mas intuitivo quando
A organização desenvolveu uma arquitetura de informação com base em princípios de segurança. As informações são de acesso restrito, porém sem autenticação claramente definida.

3 Definido quando
As informações foram claramente classificadas conforme recomendações elaboradas em critérios de confidencialidade e disponibilidade. Os usuários foram informados e treinados no tratamento das informações, desde a sua geração até a sua disposição. Porém não existe um monitoramento do acesso a informação e este é realizado com base na confiança nos colaboradores.

4 Gerenciado e Mensurável quando
As recomendações de classificação são formalmente apresentadas aos colaboradores, assim como estes são treinados e informados. A informação já possui rótulo e seu tratamento segue os padrões definidos. Existe um processo automatizado para controlar o acesso a informação.

5 Otimizado quando
A organização possui sistema automatizado para o controle de acesso a informação, com base no perfil individual de cada colaborador. Acessos indevidos são bloqueados automaticamente e notificados ao comitê de segurança da informação. Todo colaborador recebe treinamento e acompanhamento sobre o tratamento da informação.

QUESTIONÁRIO DE MATURIDADE

ORG02 – Classificação da Informação

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Informações possuem um tratamento diferenciado baseado na hierarquia funcional dos colaboradores.		X		
Existem critérios de acesso a informação	X			
O conceito de classificação da informação e sigilo é o mesmo.		X		
Maturidade Nível 2				
Existe uma arquitetura de informação com base em princípios de segurança		X		
Existem informações que são de acesso restrito.			X	
Poucas informações requerem chaves fortes de autenticação.			X	
Maturidade Nível 3				
As informações foram claramente classificadas conforme recomendações elaboradas em critérios de confidencialidade e disponibilidade				X
Os usuários foram informados e treinados no tratamento das informações, desde a sua geração até a sua disposição.				X
Existe monitoramento do acesso a informação		X		
Maturidade Nível 4				
As recomendações de classificação são formalmente apresentadas aos colaboradores.			X	
Os colaboradores são conscientizados, treinados e informados sobre a classificação da informação.				X
A informação já possui rótulo e seu tratamento segue os padrões definidos.			X	
Existe um processo automatizado para controlar o acesso a informação.			X	
Maturidade Nível 5				
Existe um sistema automatizado para o controle de acesso a informação, com base no perfil individual de cada colaborador.				X
Acessos indevidos são bloqueados automaticamente e notificados ao comitê de segurança da informação.				X
Existem indicadores da classificação da informação e de seu uso.			X	

DESCRIÇÃO DO PROCESSO

ORG03 – Segurança em Recursos Humanos

Assegurar que os colaboradores, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de furto ou roubo, fraude ou mau uso de recursos. Assegurar que colaboradores, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização. Assegurar que colaboradores, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.

OBJETIVOS DE CONTROLE

ORG03.1 – Papéis e responsabilidades
Convém que papéis e responsabilidades pela segurança da informação de colaboradores, fornecedores e terceiros sejam definidos e documentados de acordo com a política de segurança da organização.

ORG03.2 – Seleção
Convém que verificações de histórico de todos os candidatos a emprego, fornecedores e terceiros sejam realizadas de acordo com a ética, as leis e as regulamentações pertinentes, e proporcionais aos requisitos do negócio, à classificação da informações a serem acessadas e aos riscos percebidos.

ORG03.3 – Termos e condições de contratação
Como parte das suas obrigações contratuais, convém que colaboradores, fornecedores e terceiros concordem e assinemos termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidades e a da organização para a segurança da informação.

ORG03.4 – Responsabilidades da direção
Convém que a direção solicite aos colaboradores, fornecedores e terceiros que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.

ORG03.5 – Conscientização, educação e treinamento em segurança da informação
Convém que todos os colaboradores da organização e, onde pertinente, fornecedores e terceiros recebam treinamento apropriado em conscientização, atualizações regulares nas políticas e procedimentos organizacionais, relevantes para as suas funções.

ORG03.6 – Processo disciplinar
Convém que exista um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação.

ORG03.7 – Encerramento das atividades
Convém que responsabilidades para realizar o encerramento ou mudança de um trabalho sejam claramente definidas e atribuídas.

ORG03.8 – Devolução de ativos
Convém que todos os colaboradores, fornecedores e terceiros devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

ORG03.9 – Retirada de direitos de acesso
Convém que os direitos de acesso de todos os colaboradores, fornecedores e terceiros às informações e aos recursos de processamento da informação sejam retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.

MODELO DE MATURIDADE

ORG03 – Segurança em Recursos Humanos

0 Não existente quando
A organização não é sensibilizada sobre a segurança da informação sobre os recursos humanos, assim como não implementa qualquer tipo de treinamento, definição de responsabilidades ou direitos de acesso.

1 Inicial/*Ad Hoc* quando
A organização já entendeu a necessidade de tratar recursos humanos como um dos itens de segurança da informação, mas ainda de maneira simples e sem atingir toda a organização. Alguns papéis e responsabilidades são definidos, mas não formalmente atribuídos. Não existe controle de acesso ou qualquer tipo de processo disciplinar.

2 Repetível mas intuitivo quando
Papéis e responsabilidades são definidos e atribuídos, mas controlados com base na confiança dos colaboradores, fornecedores e terceiros. O processo seletivo aborda o histórico dos colaboradores que ocuparão posições sensíveis, mas de forma comedida e não restritiva. Os colaboradores são informados, mas não treinados em segurança da informação. O processo disciplinar é definido, mas não aplicado. Os direitos de acesso são removidos somente quando o departamento de recursos humanos solicita.

3 Definido quando
O processo de tratamento dos recursos humanos sobre colaboradores, fornecedores e terceiros é claramente definido e aplicado. A direção se posiciona sobre suas responsabilidades e a dos colaboradores. Treinamentos são realizados de maneira corporativa. Existe um controle de entrega e devolução de ativos para cada colaborador.

4 Gerenciado e Mensurável quando
O departamento de recursos humanos delega automaticamente acesso e ativos aos colaboradores, fornecedores e terceiros com base no perfil papel e responsabilidade individual. Existe um programa constante de treinamento e reciclagem em segurança da informação. O processo disciplinar é efetivo e aplicado. Todos os direitos de acesso são revogados automaticamente quando uma mudança ou encerramento das atividades acontece. O comitê de segurança da informação acompanha os principais indicadores do processo de maneira sistemática.

5 Otimizado quando
A organização possui um sistema de gerenciamento de identidade totalmente integrado. Os colaboradores passam por avaliações de histórico funcional e policial. O treinamento em segurança da informação é prática constante e os indivíduos que sofreram sanções disciplinares relativas a segurança da informação são reciclados quando é o caso. O encerramento de atividade é sincronizado entre a área de atuação e o departamento de recursos humanos. O comitê de segurança da informação possui poder de veto nas contratações. Acessos são monitorados e avaliados constantemente com base no perfil de cada colaborador, fornecedor ou terceiro.

QUESTIONÁRIO DE MATURIDADE

ORG03 – Segurança em Recursos Humanos

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Papéis e responsabilidades são definidos, mas não formalmente atribuídos.		X		
Os recursos humanos são tratados como itens de segurança da informação	X			
Maturidade Nível 2				
Papéis e responsabilidades são formalmente definidos e atribuídos..		X		
O processo seletivo aborda o histórico dos colaboradores para posições sensíveis		X		
O processo disciplinar é definido e fortemente aplicado	X			
Os direitos de acesso são removidos quando o RH solicita.			X	
Maturidade Nível 3				
O processo de tratamento dos recursos humanos sobre colaboradores, fornecedores e terceiros é claramente definido e aplicado.				X
A direção se posiciona sobre suas responsabilidades e a dos colaboradores.			X	
Treinamentos são realizados de maneira corporativa.				X
Existe um controle de entrega e devolução de ativos para cada colaborador.			X	
Maturidade Nível 4				
O departamento de recursos humanos delega automaticamente acesso e ativos aos colaboradores, fornecedores e terceiros com base no perfil papel e responsabilidade individual.				X
Existe um programa de treinamento em segurança da informação.			X	
O processo disciplinar é efetivo e aplicado.			X	
O comitê de segurança da informação acompanha os principais indicadores do processo de maneira sistemática.			X	
Maturidade Nível 5				
A organização possui um sistema de gerenciamento de identidade integrado.				X
Os colaboradores passam por avaliações de histórico funcional e policial.			X	
O encerramento de atividade é sincronizado entre a área de atuação e o departamento de recursos humanos.				X
O comitê de segurança da informação pode vetar contratações.				X

DESCRIÇÃO DO PROCESSO

ORG04 – Procedimentos e Responsabilidades Operacionais

Garantir a operação segura e correta dos recursos de processamento da informação. Convém que os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações sejam definidos. Isso abrange o desenvolvimento de procedimentos operacionais apropriados.

OBJETIVOS DE CONTROLE

ORG04.1 – Documentação dos procedimentos de operação
Convém que os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.

ORG04.2 – Gestão de mudanças
Convém que modificações nos recursos de processamento da informação e sistemas sejam controladas.

ORG04.3 – Segregação de funções
Convém que funções e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.

ORG04.4 – Separação dos recursos de desenvolvimento, teste e de produção
Convém que recursos de desenvolvimento, teste e produção sejam separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

MODELO DE MATURIDADE

ORG04 – Procedimentos e Responsabilidades Operacionais

0 Não existente quando
Os procedimentos de operação são conhecidos, mas não são documentados. A organização não faz o controle e gestão de mudanças, assim como não existe segregação de funções ou ambientes específicos para desenvolvimento e produção.

1 Inicial/*Ad Hoc* quando
Alguns procedimentos operacionais já são documentados, mas não são revisados ou atualizados. A organização possui uma visão de mudanças, mas sem a implantação de um controle real.

2 Repetível mas intuitivo quando
Todos os procedimentos operacionais evoluíram para um estágio onde são seguidos por diferentes pessoas fazendo a mesma tarefa. Algumas funções foram segregadas a fim de se obter maior controle, principalmente sobre mudanças e operação. Os ambientes de desenvolvimento e produção foram separados, mas não seguem critérios rígidos de controle.

3 Definido quando
Todos os procedimentos foram padronizados, documentados e comunicados através de treinamento. A gestão de mudanças foi documentada e as vezes seguida. A segregação de funções é formalmente definida, mas ainda com dificuldades de implantação. Os ambientes de desenvolvimento e produção são bem distintos.

4 Gerenciado e Mensurável quando
O comitê de segurança da informação já coordena a segregação de funções e todas as mudanças são monitoradas por ele. Foi incluído um ambiente exclusivo para teste entre os ambientes de desenvolvimento e produção. Os procedimentos operacionais são documentados, treinados e monitorados.

5 Otimizado quando
Os procedimentos operacionais são testados e revisados constantemente. Os colaboradores entendem e adotam a segregação de funções de maneira natural e se reportam com facilidade aos responsáveis diretos. Toda e qualquer mudança é controlada e monitorada. Os ambientes de desenvolvimento e testes utilizam informações devidamente alteradas para evitar vazamento de informações sensíveis e para não provocar danos no ambiente de produção.

QUESTIONÁRIO DE MATURIDADE

ORG04 – Procedimentos e Responsabilidades Operacionais

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Os procedimentos operacionais são documentados, mas não são revisados ou atualizados.		X		
Existe um controle sobre mudanças nos ambientes.	X			
Maturidade Nível 2				
Os procedimentos operacionais evoluíram para um estágio onde são seguidos por diferentes pessoas fazendo a mesma tarefa		X		
Funções foram segregadas a fim de se obter maior controle, principalmente sobre mudanças e operação.		X		
Os ambientes de desenvolvimento e produção foram separados		X		
Maturidade Nível 3				
Os procedimentos foram padronizados, documentados e comunicados através de treinamento.				X
A gestão de mudanças está documentada e implementada.		X		
Os ambientes de desenvolvimento e produção são bem distintos.				X
Maturidade Nível 4				
O comitê de segurança da informação coordena a segregação de funções e todas as mudanças são monitoradas por ele				X
Existe um ambiente exclusivo para testes entre os ambientes de desenvolvimento e produção			X	
Os procedimentos operacionais são documentados, treinados e monitorados ativamente.			X	
Maturidade Nível 5				
Os procedimentos operacionais são testados e revisados constantemente.				X
Os colaboradores entendem e adotam a segregação de funções de maneira natural.			X	
Toda e qualquer mudança é controlada e monitorada.				X
Os ambientes de desenvolvimento e testes utilizam informações devidamente alteradas para evitar vazamento de informações sensíveis.			X	

DESCRIÇÃO DO PROCESSO

ORG05 – Troca de Informações

Assegurar a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas. Convém que as trocas de informações e softwares entre organizações estejam baseadas numa política formal específica, sejam efetuadas a partir de acordos entre as partes e estejam em conformidade com toda a legislação pertinente.

OBJETIVOS DE CONTROLE

ORG05.1 – Políticas e procedimentos para troca de informações
Convém que políticas, procedimentos e controles sejam estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação.

ORG05.2 – Acordos para troca de informações
Convém que sejam estabelecidos acordos para a troca de informações e softwares entre a organização e entidades externas.

ORG05.3 – Mídias em trânsito
Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externo aos limites físicos da organização.

ORG05.4 – Mensagens eletrônicas
Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.

ORG05.5 – Sistemas de informações do negócio
Convém que políticas e procedimentos sejam desenvolvidos e implementados para proteger as informações associadas com a interconexão de sistemas de informação do negócio.

MODELO DE MATURIDADE

ORG05 – Troca de Informações

0 Não existente quando
A organização não está sensibilizada em proteger informações durante as trocas com partes externas, assim como não possui qualquer tipo de proteção para as mensagens eletrônicas e sistemas de informação.

1 Inicial/*Ad Hoc* quando
Foram estabelecidos alguns procedimentos para a troca de informações, mas são raramente seguidos. Não existe um acordo formal entre a organização e entidades externas no que diz respeito a troca de informações. As mensagens eletrônicas são protegidas por iniciativas de apenas alguns colaboradores.

2 Repetível mas intuitivo quando
A organização estabeleceu procedimentos de troca de informações, mas de maneira pontual. Acordos de troca de informações com entidades externas são mais claros e seguidos. Os sistemas de informação já possuem alguns controles de acesso e proteção das informações.

3 Definido quando
A organização definiu e formalizou políticas e procedimentos de troca de informações, mas não implementou nenhum tipo de gerenciamento e monitoramento. Os acordos de troca de informações já fazem parte dos contratos com entidades externas. Foram implementadas ferramentas para proteger as mensagens eletrônicas e os sistemas de informação.

4 Gerenciado e Mensurável quando
O comitê de segurança da informação monitora os contratos e acordos de trocas de informação da organização, conforme as políticas definidas e treinadas. Já existem indicadores relacionados a proteção das mensagens eletrônicas e sistemas de informação.

5 Otimizado quando
A organização somente realiza troca de informações com entidades que entendem e praticam a política e procedimentos estabelecidos para a troca de informações inclusive com os procedimentos de monitoramento por parte da organização. As ferramentas de proteção de mensagens eletrônicas e sistemas de informação estão automatizadas e são constantemente monitoradas. Indicadores sobre estas ferramentas auxiliam a tomada de decisão realizada pelo comitê de segurança da informação.

QUESTIONÁRIO DE MATURIDADE

ORG05 – Troca de Informações

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem procedimentos para a troca de informações		X		
Existe um acordo com as entidades externas para a troca de informações	X			
As mensagens eletrônicas são protegidas	X			
Maturidade Nível 2				
Existe um acordo com as entidades externas para a troca de informações			X	
Existem controles de acesso e proteção das informações		X		
As mensagens eletrônicas são protegidas			X	
Maturidade Nível 3				
Estão definidas e formalizadas políticas e procedimentos de troca de informações.				X
Os acordos de troca de informações fazem parte dos contratos com entidades externas				X
Existem ferramentas para proteger as mensagens eletrônicas e os sistemas de informação.			X	
Os colaboradores são devidamente treinados na troca das informações.			X	
Maturidade Nível 4				
O comitê de segurança da informação monitora os contratos e acordos de trocas de informação da organização.				X
Existem indicadores relacionados a proteção das mensagens eletrônicas e sistemas de informação.			X	
Existe um programa de conscientização sobre a troca de informações.			X	
Maturidade Nível 5				
A organização somente realiza troca de informações com entidades que entendem e praticam a política para a troca de informações.			X	
As ferramentas de proteção de mensagens eletrônicas e sistemas de informação estão automatizadas.				X
Indicadores sobre estas ferramentas auxiliam a tomada de decisão realizada pelo comitê de segurança da informação.			X	

DESCRIÇÃO DO PROCESSO

ORG06 – Requisitos de Negócio para Controle de Acesso

Controlar acesso à informação. Convém que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação.

OBJETIVOS DE CONTROLE

ORG06.1 – Política de controle de acesso

Convém que a política de controle de acesso seja estabelecida documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e segurança da informação.

MODELO DE MATURIDADE

ORG06 – Requisitos de Negócio para Controle de Acesso

0 Não existente quando
A organização não utiliza nenhum tipo de política de controle de acesso.

1 Inicial/*Ad Hoc* quando
A organização já utiliza alguns critérios de controle de acesso, mas de maneira pontual e apenas com a visão sistêmica.

2 Repetível mas intuitivo quando
Um esboço de política de acesso foi formulado, os critérios de concessão de acesso já levam em conta os requisitos de negócio, porém de maneira informal e sem qualquer tipo de gerenciamento.

3 Definido quando
A organização possui uma política formal de controle de acesso, totalmente baseada nos requisitos de negócio e na segurança da informação. Os colaboradores são informados e a política é pública e bem comunicada. Por outro lado não existe um gerenciamento sobre como é executada ou controlada a política e quais são seus resultados.

4 Gerenciado e Mensurável quando
A política de acesso é gerenciada e monitorada pelo comitê de segurança da informação. Os colaboradores são formalmente comunicados e treinados em relação a política. Alguns indicadores de desempenho foram desenvolvidos, relacionando a política e a aderência de sua aplicação.

5 Otimizado quando
A política de controle de acesso periodicamente passa por um processo de análise crítica, adequando-se aos requisitos de negócio. Os colaboradores-chave participam de maneira profunda na identificação dos requisitos de negócio e de segurança da informação e na representação destes na política de acesso.

QUESTIONÁRIO DE MATURIDADE

ORG06 – Requisitos de Negócio para Controle de Acesso

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem critérios de controle de acesso ao negócio		X		
O negócio oferece requisitos de controle aos sistemas	X			
Maturidade Nível 2				
Critérios de concessão de acesso já levam em conta os requisitos de negócio		X		
Existe uma política de acesso as informações e sistemas		X		
Maturidade Nível 3				
Existe uma política formal de controle de acesso, totalmente baseada nos requisitos de negócio e na segurança da informação.			X	
Os colaboradores são informados e a política é pública e comunicada.				X
Maturidade Nível 4				
A política de acesso é gerenciada e monitorada pelo comitê de segurança da informação.				X
Os colaboradores são formalmente comunicados e treinados em relação a política			X	
Indicadores de desempenho foram desenvolvidos, relacionando a política e a aderência de sua aplicação			X	
Maturidade Nível 5				
A política de controle de acesso periodicamente passa por um processo de análise crítica, adequando-se aos requisitos de negócio.				X
Os colaboradores-chave participam de maneira profunda na identificação dos requisitos de negócio e de segurança da informação e na representação destes na política de acesso.				X
A política é vista como parte da visão institucional.			X	

DESCRIÇÃO DO PROCESSO

ORG07 – Responsabilidade dos Usuários

Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou furto da informação e dos recursos de processamento de informação.

OBJETIVOS DE CONTROLE

ORG07.1 – Uso de senhas

Convém que os usuários sejam solicitados a seguir as boas práticas de segurança da informação na seleção e uso de senhas.

ORG07.2 – Equipamento de usuário sem monitoração

Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.

ORG07.3 – Política de mesa limpa e tela limpa

Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removível e política de tela limpa para os recursos de processamento da informação.

MODELO DE MATURIDADE

ORG07 – Responsabilidade dos Usuários

0 Não existente quando
A organização não exige senha dos usuários e os equipamentos não possuem qualquer tipo de controle, monitoramento ou gerenciamento.

1 Inicial/*Ad Hoc* quando
Os usuários já possuem senhas, mas sem critérios definidos para seu uso e guarda. Os equipamentos são apenas registrados para os usuários, sendo que estes possuem total autonomia sobre seu uso e disposição.

2 Repetível mas intuitivo quando
Já existem critérios para a definição de senhas, mas seu uso depende da motivação dos usuários. Alguns equipamentos mais críticos são monitorados, mas sem seguir um padrão.

3 Definido quando
Os procedimentos de tratamento de senhas são formais e informados a todos os usuários, mas ainda não existe uma ferramenta que controle isso automaticamente. Políticas de mesa limpa e tela limpa foram definidas e comunicadas.

4 Gerenciado e Mensurável quando
A organização já possui uma ferramenta que inibe o mau uso de senhas, forçando os usuários s seguir os critérios estabelecidos. Os computadores não monitorados possuem *software* de segurança que inibe a instalação de outros softwares ou mudança no perfil dos usuários. As políticas de mesa limpa e tela limpa são formalmente treinadas e monitoradas.

5 Otimizado quando
A troca de senhas segue a política de segurança da informação da organização e todos os usuários são monitorados. Existem indicadores relacionados com a geração de senhas e das tentativas de utilização de senhas antigas. Os usuários seguem a política de mesa limpa e tela limpa, passando por controles internos rígidos e que norteiam os treinamentos de conscientização.

QUESTIONÁRIO DE MATURIDADE

ORG07 – Responsabilidade dos Usuários

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
A responsabilidade do uso de senhas é dos colaboradores.		X		
O uso dos equipamentos segue critérios de bom senso.	X			
Maturidade Nível 2				
Existem critérios para a definição de senhas, e seu uso é de responsabilidade dos colaboradores.			X	
Equipamentos mais críticos são monitorados, mas sem seguir um padrão.			X	
Maturidade Nível 3				
Os procedimentos de tratamento de senhas são formais e informados a todos os colaboradores.				X
Políticas de mesa limpa e tela limpa foram definidas e comunicadas.				X
Ações de conscientização sobre senhas e seu uso são periódicas.			X	
Maturidade Nível 4				
As senhas são controladas por ferramentas automatizadas.				X
Os computadores não monitorados possuem software de segurança que inibe a instalação de outros softwares ou mudança no perfil dos colaboradores.			X	
As políticas de mesa limpa e tela limpa são formalmente treinadas e monitoradas.				X
Maturidade Nível 5				
A troca de senhas segue a política de segurança da informação da organização e todos os colaboradores são monitorados				X
Existem indicadores relacionados com a geração de senhas e das tentativas de utilização de senhas antigas.				X
Os colaboradores seguem a política de mesa limpa e tela limpa, passando por controles internos rígidos e que norteiam os treinamentos de conscientização.			X	

DESCRIÇÃO DO PROCESSO

ORG08 – Requisitos de Segurança de Sistemas de Informação

Garantir que segurança é parte integrante de sistemas de informação. Sistemas de informação incluem sistemas operacionais, infraestrutura, aplicações de negócios, produtos de prateleira, serviços e aplicações desenvolvidas pelo usuário.

OBJETIVOS DE CONTROLE

ORG08.1 – Análise e especificação dos requisitos de segurança

Convém que sejam especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes.

MODELO DE MATURIDADE

ORG08 – Requisitos de Segurança de Sistemas de Informação

0 Não existente quando
A organização não estabelece nenhum tipo de requisito de segurança para os sistemas de informação, tanto para os novos como para ou já existentes.

1 Inicial/*Ad Hoc* quando
Alguns requisitos de segurança já são estabelecidos, mas com base na experiência dos usuários e não na operação de negócio. Mesmo assim apenas em pontos específicos e que não representam uma análise cuidadosa de riscos.

2 Repetível mas intuitivo quando
Vários requisitos de segurança são utilizados por vários colaboradores, mas de maneira intuitiva e sem controle. A aquisição de novos sistemas já seguem requisitos de segurança, mas sem uma formalidade definida.

3 Definido quando
Os requisitos de segurança em sistemas são claramente definidos e comunicados, por mais que sua aplicação não seja controlada, assim como seu impacto no negócio. Os sistemas existentes passam por estudos de melhorias com base nos requisitos de segurança definidos.

4 Gerenciado e Mensurável quando
O comitê de segurança da informação monitora a aquisição de novos sistemas de informação, buscando aderência aos requisitos de segurança definidos. As melhorias nos sistemas atuais são projetadas levando em conta os requisitos. Alguns indicadores de aderência aos requisitos são aplicados.

5 Otimizado quando
Todos os sistemas de informação respeitam os requisitos de segurança, passando por análises críticas independentes e testes de penetração. O comitê de segurança da informação possui controle sobre os sistemas da organização e o mapeamento de suas fragilidades.

QUESTIONÁRIO DE MATURIDADE

ORG08 – Requisitos de Segurança de Sistemas de Informação

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Requisitos de segurança são estabelecidos, mas com base na experiência dos colaboradores.		X		
Análises de riscos são realizadas mediante solicitações.		X		
Maturidade Nível 2				
Requisitos de segurança são utilizados por vários colaboradores, mas de maneira intuitiva e sem controle.			X	
A aquisição de novos sistemas já seguem requisitos de segurança, mas sem uma formalidade definida.		X		
Maturidade Nível 3				
Os requisitos de segurança em sistemas são claramente definidos e comunicados.				X
Os sistemas existentes passam por estudos de melhorias com base nos requisitos de segurança definidos.			X	
As análises de impacto no negócio são pontuais e refletem necessidades específicas.		X		
Maturidade Nível 4				
O comitê de segurança da informação monitora a aquisição de novos sistemas de informação.				X
As melhorias nos sistemas atuais são projetadas levando em conta os requisitos de segurança da informação.			X	
Indicadores de aderência aos requisitos são aplicados aos sistemas.			X	
Maturidade Nível 5				
Todos os sistemas de informação respeitam os requisitos de segurança, passando por análises críticas independentes e testes de penetração.				X
O comitê de segurança da informação possui controle sobre os sistemas da organização e o mapeamento de suas fragilidades.			X	
As análises de impacto são extensivas e refletem as operações de negócio.			X	

DESCRIÇÃO DO PROCESSO

FIS01 – Áreas Seguras

Este processo tem como objetivo prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização através de definição de perímetros de segurança com a aplicação de controles de entrada e saída em cada fronteira destes perímetros, estabelecendo os procedimentos operacionais para os mesmos.

OBJETIVOS DE CONTROLE

FIS01.1 – Perímetro de segurança física

Convém que sejam utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento de informações.

FIS01.2 – Controles de entrada física

Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

FIS01.3 – Segurança em escritórios, salas e instalações

Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.

FIS01.4 – Proteção contra ameaças externas e do meio ambiente

Convém que sejam projetadas e aplicadas proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.

FIS01.5 – Trabalhando em áreas seguras

Convém que seja projetada e aplicada proteção física, bom como diretrizes para o trabalho em áreas seguras.

FIS01.6 – Acesso do público, áreas de entrega e de carregamento

Convém que os pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.

MODELO DE MATURIDADE

FIS01 – Áreas Seguras

0 Não existente quando
A organização não segmenta as áreas físicas e perímetros, assim como não estabelece pontos de acesso e controle.

1 Inicial/*Ad Hoc* quando
São estabelecidos perímetros físicos, mas com pouco ou nenhum controle de acesso. Portas e portões de acesso possuem placas de avisos em relação ao acesso restrito. Controles de acesso são aplicados individualmente em casos específicos.

2 Repetível mas intuitivo quando
Os acessos externos a organização são controlados e registrados em todas as portarias e entradas. Porém internamente os perímetros não são definidos com clareza e os colaboradores não possuem treinamento específico sobre os procedimentos de acesso e as responsabilidades. Os controles de acesso a salas e instalações estão baseados na confiança pessoal, através de chaves de portas e cofres.

3 Definido quando
Todos os perímetros estão definidos e os critérios de acesso são de conhecimento de todos através de comunicação formal e escrita. Existem controles em todos os limites de perímetros. Responsabilidades foram definidas e atribuídas. Procedimentos de acesso e segurança foram estabelecidos e treinados. Os procedimentos não são sofisticados mas existe a formalização das práticas existentes.

4 Gerenciado e Mensurável quando
Os pontos de controle de acesso são monitorados e os acessos são verificados em todas as situações. Existe gerenciamento sobre as atividades executadas, buscando identificar falhas e suas correções. Os programas de treinamento são constantes e buscam a melhoria da cultura organizacional. Alguns dos pontos de controle utilizam ferramentas automatizadas de uma maneira limitada ou fragmentada. Foram criados indicadores de desempenho para avaliar os controles estabelecidos.

5 Otimizado quando
As atividades de controle são constantemente avaliadas e melhoradas, assim como estão altamente aderente a norma de segurança ISO/IEC 27002:2007. As atividades chegaram a um nível de aprimoramento que refletem as ações de monitoramento e gerenciamentos dos indicadores. Responsabilidades foram atribuídas e constantemente avaliadas. Os controles são automatizados em sua totalidade, gerando indicadores específicos e complementares aos do processo. A organização suporta mudanças com velocidade, eficiência e eficácia.

QUESTIONÁRIO DE MATURIDADE

FIS01– Áreas Seguras

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
A organização possui alguns controles de acesso em portas e portões.	X			
Existem placas e avisos informando sobre acesso restrito.	X			
É possível diferenciar perímetros físicos de segurança.	X			
A entrada da organização é livre, sem necessidade de identificação.			X	
Maturidade Nível 2				
Os acessos são autenticados e autorizados em todas as entradas externas.			X	
Os acessos são autenticados e autorizados em todas as entradas internas.		X		
Existe uma política de acessos e os colaboradores são treinados na integração inicial (quando contratados).			X	
O uso de chaves nas portas é de responsabilidade compartilhada.			X	
Maturidade Nível 3				
Existe uma política forte de controle de acesso (formalmente comunicada)				X
Os perímetros de segurança física são claros e controlados.			X	
Os colaboradores são treinados sobre segurança física e existe o papel de "key user" para a multiplicação e conscientização sobre a segurança.				X
Maturidade Nível 4				
Existe monitoração reativa e proativa nos controles de acesso.			X	
Existem revisões periódicas dos controles de acesso dos registros de acesso.				X
Alguns pontos de controle já são automatizados.		X		
Existem metas de controle a serem alcançadas pelas equipes de segurança.		X		
Maturidade Nível 5				
O processo de controle de acesso possui alto grau de automatização.				X
Reuniões de avaliação dos indicadores de acesso acontecem periodicamente e as metas são constantemente reportadas a alta gestão.			X	
O gerenciamento de acesso físico é forte e responde com agilidade a eventos e mudanças estratégicas.				X

DESCRIÇÃO DO PROCESSO

FIS02 – Segurança em Equipamentos

Este processo tem como objetivo impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das atividades da organização através da instalação de proteções nos equipamentos, tanto para falhas de energia como para alocação em local seguro e acesso não autorizado.

OBJETIVOS DE CONTROLE

FIS02.1 – Instalação e proteção do equipamento
Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

FIS02.2 – Utilidades
Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

FIS02.3 – Segurança do cabeamento
Convém que o cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações seja protegido contra interceptação ou danos.

FIS02.4 – Manutenção dos equipamentos
Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanentes.

FIS02.5 – Segurança de equipamentos fora das dependências da organização
Convém que sejam tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

FIS02.6 – Reutilização e alienação segura de equipamentos
Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre gravados com segurança.

FIS02.7 – Remoção de propriedade
Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.

MODELO DE MATURIDADE

FIS02 – Segurança em Equipamentos

0 Não existente quando
A organização não controla os equipamentos em relação a sua segurança física e técnica. Não há controle do conteúdo dos equipamentos e das instalações de infraestrutura.

1 Inicial/*Ad Hoc* quando
Existem evidências que a organização reconheceu que existe necessidade de proteger os equipamentos de rede. No entanto, as atividades de proteção não fazem parte de processos definidos e são executadas conforme a experiência e disponibilidade dos colaboradores. O único controle existente é a relação de equipamentos a serem protegidos e algumas das soluções aplicadas. As principais ações são referentes a instalação e manutenção dos equipamentos.

2 Repetível mas intuitivo quando
As ações de proteção aos equipamentos já são mais padronizadas e todos os colaboradores utilizam a mesma metodologia. O treinamento dos colaboradores para a execução das tarefas é informal, geralmente acompanhando um colaborador mais experiente. Existem instruções de trabalho que não são monitoradas e fica a cargo de cada colaborador o seu cumprimento. Há um alto grau de confiança no conhecimento dos indivíduos e consequentemente erros podem ocorrer. Além da instalação e manutenção dos equipamentos, já existe a alocação de propriedade e definições de segurança para equipamentos que estejam fora das dependências da organização.

3 Definido quando
Todos os procedimentos de segurança em equipamentos estão padronizados, descritos e formalmente apresentados em documentos controlados. Cada equipamento possui formalmente um proprietário, com a respectiva folha de controle preenchida e assinada. Os procedimentos de segurança são formalmente treinados e registrados os desempenhos dos colaboradores. A organização estabeleceu controles físicos para o cabeamento estruturado da rede lógica. Ainda não existe uma forma de gerenciamento e medição de desempenho do processo.

4 Gerenciado e Mensurável quando
Foram desenvolvidos métodos de gerenciamento e monitoramento do processo, visando a aderência entre o documentado e o executado, possibilitando ações corretivas e preventivas. Além disso, o processo passa pelo ciclo de melhoria contínua e alinhamento com a norma de segurança da informação. Algumas atividades conseguem ser executadas através de procedimentos automatizados, como integração entre o RH e as folhas de propriedade, mas na maioria das vezes as ferramentas são utilizadas de uma maneira limitada.

5 Otimizado quando
O processo foi refinado a um nível de boas práticas internacionais, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade como outras organizações. A segurança dos equipamentos, assim como a responsabilidade pelos mesmos utiliza um caminho integrado com os sistemas de informação da organização. Todo colaborador é treinado em relação ao seu papel como agente de segurança, tanto sobre o equipamento como sobre a infraestrutura. As informações de gerenciamento apoiam assertivamente as decisões da organização de forma a uma rápida adequação quando necessário.

QUESTIONÁRIO DE MATURIDADE

FIS02 – Segurança em Equipamentos

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Os equipamentos são inventariados.			X	
Existe um plano de manutenção preventiva de equipamentos de rede.			X	
Equipamentos possuem proteção contra roubo, furto ou dano.	X			
Maturidade Nível 2				
A proteção dos equipamentos segue um padrão único.			X	
Os colaboradores responsáveis pela proteção sofrem algum tipo de treinamento e seguem instruções de trabalho padrão.		X		
Existe alocação de propriedade nos equipamentos.		X		
Existe controle dos equipamentos fora das dependências da organização.		X		
Maturidade Nível 3				
O procedimento de segurança dos equipamentos é formalmente comunicado e treinado aos colaboradores				X
Cada equipamento possui formalmente um proprietário.			X	
A organização estabeleceu controles físicos para o cabeamento estruturado da rede lógica.			X	
Existe um procedimento de auditoria dos equipamentos.	X			
Maturidade Nível 4				
Existe um procedimento periódico de auditoria dos equipamentos.			X	
Existe automatização nos controles dos equipamentos.		X		
Existem e são aplicadas penalizações quando não conformidades são detectadas.			X	
Maturidade Nível 5				
Existem metas e métricas de gerenciamento da segurança dos equipamentos			X	
O processo de controle é gerenciado e medido com regularidade.				X
A automatização é alta no controle dos equipamentos.				X
O treinamento de colaboradores é constante, assim como os programas de conscientização em relação a segurança e responsabilidade.			X	

DESCRIÇÃO DO PROCESSO

TEC01 – Gerenciamento de Serviços de Terceiros

Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados. Convém que a organização verifique a implementação dos acordos, monitore a conformidade com tais acordos e gerencie as mudanças para garantir que os serviços entregues atendem a todos os requisitos acordados com os terceiros.

OBJETIVOS DE CONTROLE

TEC01.1 – Entrega de serviços

Convém que seja garantido que os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro.

TEC01.2 – Monitoramento e análise crítica de serviços terceirizados

Convém que os serviços, relatórios e registros fornecidos por terceiro sejam regularmente monitorados e analisados criticamente, e que auditorias sejam executadas regularmente.

TEC01.3 – Gerenciamento de mudanças para serviços terceirizados

Convém que mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, procedimentos e controles existentes, sejam gerenciados levando-se em conta a criticidade dos sistemas e processos de negócio envolvidos e a reanálise/reavaliação de riscos.

MODELO DE MATURIDADE

TEC01 – Gerenciamento de Serviços de Terceiros

0 Não existente quando
Não existe controles sobre os serviços de terceiros que estejam relacionados com as operações de negócio ou com a segurança da informação.

1 Inicial/*Ad Hoc* quando
Alguns serviços de terceiros são baseados em acordos de nível de serviço e em termos de confidencialidade, mas mesmo assim de maneira pontual e dependente dos colaboradores internos. Os acordos não são monitorados, assim como também não são monitoradas as mudanças sobre os serviços terceirizados.

2 Repetível mas intuitivo quando
Os serviços terceirizados são entregues com base em critérios informais de segurança da informação, sendo que em casos bem específicos existem controles e análises do nível de serviço. Algumas mudanças não são permitidas sem os devidos processos de gerenciamento de mudanças.

3 Definido quando
A segurança na entrega de serviços de terceiros é definida e comunicada. Além disso, cláusulas de segurança são colocadas em contratos, mas sem o devido gerenciamento. A organização estabeleceu critérios de monitoramento nos serviços mais críticos e solicita dos terceiros relatórios de segurança. O gerenciamento de mudanças é realizado de maneira simples, manual e sem muita integração com os terceiros.

4 Gerenciado e Mensurável quando
Existem indicadores relacionados com a entrega de serviços de terceiros, buscando avaliar a segurança da informação. Critérios de controle de segurança são informados aos terceiros, assim como é fornecido treinamento. Os processos de gerenciamento de mudanças são bem definidos para os terceiros e relacionado com cláusulas contratuais.

5 Otimizado quando
A entrega de serviços de terceiros é totalmente gerenciada e segue as políticas de segurança da informação da organização. Os acordos de segurança são monitorados e auditorias nos terceiros são acordadas e realizadas. Os terceiros possuem comprometimento claro com o gerenciamento de mudanças e os processos são avaliados dentro do perfil de criticidade e riscos de cada serviço.

QUESTIONÁRIO DE MATURIDADE

TEC01 – Gerenciamento de Serviços de Terceiros

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Serviços de terceiros são baseados em acordos de nível de serviço e em termos de confidencialidade.		X		
O controle sobre mudanças nos serviços de terceiros depende dos colaboradores internos.	X			
Maturidade Nível 2				
Os serviços terceirizados são entregues com base em critérios informais de segurança da informação.		X		
Existem controles e análises do nível de serviço.		X		
Mudanças não são permitidas sem os devidos processos de gerenciamento de mudanças.		X		
Maturidade Nível 3				
A segurança na entrega de serviços de terceiros é definida e comunicada. Treinamento e conscientização são realizados periodicamente.				X
Cláusulas de segurança são colocadas em contratos.			X	
A organização estabeleceu critérios de monitoramento nos serviços mais críticos e solicita dos terceiros relatórios de segurança			X	
O gerenciamento de mudanças é realizado de maneira simples.			X	
Maturidade Nível 4				
Existem indicadores relacionados com a entrega de serviços de terceiros, buscando avaliar a segurança da informação.				X
Critérios de controle de segurança são informados aos terceiros, assim como é fornecido treinamento.			X	
Os processos de gerenciamento de mudanças são bem definidos para os terceiros e relacionado com cláusulas contratuais.			X	
Maturidade Nível 5				
A entrega de serviços de terceiros é totalmente gerenciada e segue as políticas de segurança da informação da organização.				X
Os acordos de segurança são monitorados e auditorias nos terceiros são acordadas e realizadas.			X	

DESCRIÇÃO DO PROCESSO

TEC02 – Planejamento e Aceitação dos Sistemas

Minimizar o risco de falhas nos sistemas. O planejamento e a preparação prévios são requeridos para garantir a disponibilidade adequada de capacidade e recursos para entrega do desempenho desejado ao sistema.

OBJETIVOS DE CONTROLE

TEC02.1 – Gestão de capacidade

Convém que a utilização dos recursos seja monitorada e ajustada, e as projeções feitas para necessidades de capacidade futura, para garantir o desempenho requerido do sistema.

TEC02.2 – Aceitação de sistemas

Convém que sejam estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões, e que sejam efetuados testes apropriados do(s) sistemas(s) durante seu desenvolvimento e antes da sua aceitação.

MODELO DE MATURIDADE

TEC02 – Planejamento e Aceitação dos Sistemas

0 Não existente quando
A organização não faz nenhum tipo de controle sobre os sistemas e suas capacidades de operação.

1 Inicial/*Ad Hoc* quando
Alguns sistemas já possuem critérios simples de aceitação, mas sua aplicação é dependente do colaborador. A capacidade dos sistemas é estimada em comparações com o mercado.

2 Repetível mas intuitivo quando
Foram definidos procedimentos gerais para o aceite de sistemas, de maneira a controlar seus testes e homologações. Os colaboradores aplicam os critérios sob sua própria responsabilidade. Os sistemas em produção são monitorados, buscando identificar erros e falhas operacionais, mas sem o objetivo de mensurar desempenho ou capacidade.

3 Definido quando
O gerenciamento de capacidade dos sistemas se tornou um processo formal, definido e comunicado a todos os colaboradores pertinentes. O gerenciamento e monitoração dos sistemas são realizados de maneira manual, mas controlada. Foram definidos critérios formais para a aceitação de sistemas, tanto novos como os atualizados. Os colaboradores foram treinados e seguem os procedimentos com o máximo de aderência possível.

4 Gerenciado e Mensurável quando
Os sistemas de gerenciamento e monitoração de sistemas são automatizados e fornece indicadores em tempo real. Os indicadores já auxiliam na tomada de decisão por serem confiáveis e íntegros. Além disso, estão relacionados com os critérios de aceitação de sistemas definidos. Os processos passam por análises críticas internas e com isso passam por um constante aprimoramento.

5 Otimizado quando
Os indicadores de gestão de capacidade auxiliam no planejamento estratégico de segurança da informação e no planejamento estratégico de tecnologia da informação. Além disso, auxiliam no ajuste dos planos de continuidade de negócios e recuperação de desastres. A aceitação de sistemas é integrada com o banco de dados de configuração, fornecendo informações vitais para os processos de gestão de incidentes e gestão de mudanças. Análises críticas independentes acontecem periodicamente sobre a gestão de capacidade e aceitação de sistemas.

QUESTIONÁRIO DE MATURIDADE

TEC02 – Planejamento e Aceitação dos Sistemas

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Os sistemas já possuem critérios simples de aceitação		X		
A capacidade dos sistemas é estimada em comparações com o mercado.	X			
Maturidade Nível 2				
Existem definidos procedimentos gerais para o aceite de sistemas.			X	
Os colaboradores aplicam os critérios sob sua própria responsabilidade.		X		
Os sistemas em produção possuem monitoração.			X	
A capacidade dos sistemas é estimada através de estatísticas internas.			X	
Maturidade Nível 3				
O gerenciamento de capacidade dos sistemas se tornou um processo formal, definido e comunicado a todos os colaboradores pertinentes.				X
O gerenciamento e monitoração dos sistemas são realizados de maneira manual, mas controlada.			X	
Existem critérios formais para a aceitação de sistemas, tanto novos como os atualizados.			X	
Maturidade Nível 4				
Os sistemas de gerenciamento e monitoração de sistemas são automatizados e fornece indicadores em tempo real.				X
Os indicadores auxiliam na tomada de decisão e estão relacionados com os critérios de aceitação de sistemas definidos.			X	
Os processos passam por análises críticas internas.			X	
Maturidade Nível 5				
Os indicadores de gestão de capacidade auxiliam no planejamento estratégico de segurança da informação e de TI			X	
Os indicadores de gestão de capacidade auxiliam no ajuste dos planos de continuidade de negócios.				X
Análises críticas independentes acontecem periodicamente sobre a gestão de capacidade e aceitação de sistemas.				X

DESCRIÇÃO DO PROCESSO

TEC03 – Proteção contra Códigos Maliciosos e Códigos Móveis

Proteger a integridade do software e da informação. Precauções são requeridas para prevenir e detectar a introdução de códigos maliciosos e códigos móveis não autorizados.

OBJETIVOS DE CONTROLE

TEC03.1 – Controle contra códigos maliciosos

Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

TEC03.2 – Controles contra códigos móveis

Onde o uso de códigos móveis é autorizado, convém que a configuração garanta que o código móvel autorizado opere de acordo com uma política de segurança da informação claramente definida e códigos móveis não autorizados tenham sua execução impedida.

MODELO DE MATURIDADE

TEC03 – Proteção contra Códigos Maliciosos e Códigos Móveis

0 Não existente quando
A organização não possui qualquer tipo de controle sobre códigos maliciosos ou móveis. Nem mesmo os usuários são informados ou treinados sobre o assunto.

1 Inicial/*Ad Hoc* quando
A organização possui ferramentas de controles para controlar códigos maliciosos, mas sua aplicação e eficácia estão associadas ao perfil dos colaboradores, não possuindo controle centralizado. Estas ferramentas são baseadas nas assinaturas de software. Os usuários são orientados de maneira reativa em relação aos cuidados necessários para o correto tratamento de códigos maliciosos e móveis.

2 Repetível mas intuitivo quando
As ferramentas de controle utilizadas para detectar códigos maliciosos e móveis são aplicadas em todos os ambientes de trabalho e com atuação e dependência indireta dos colaboradores. Alguns treinamentos e ações de conscientização existem de maneira pontual e a efetividade do processo está concentrada no colaborador.

3 Definido quando
Todos os colaboradores passam por treinamentos e workshops periódicos visando conscientização sobre o tema. As ferramentas de controle possuem administração centralizada. As aplicações que possuem códigos móveis emitem mensagens que auxiliam os colaboradores no seu uso seguro.

4 Gerenciado e Mensurável quando
São gerados indicadores de atuação das ferramentas de controle de códigos maliciosos e móveis. Os colaboradores são avaliados periodicamente sobre o uso das aplicações e seus riscos. As ferramentas de controle bloqueiam os códigos desconhecidos, aumentando a segurança da informação.

5 Otimizado quando
O comitê de segurança da informação utiliza destes indicadores para a tomada de ações corretivas e elaboração de projetos estratégicos. Os usuários possuem uma ferramenta de comunicação, onde solicitam a avaliação e liberação de códigos móveis relacionados as operações de negócio.

QUESTIONÁRIO DE MATURIDADE

TEC03 – Proteção contra Códigos Maliciosos e Códigos Móveis

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem ferramentas de controles para controlar códigos maliciosos.		X		
As ferramentas são baseadas nas assinaturas de software.	X			
Os usuários são orientados de maneira reativa em relação aos cuidados necessários para o correto tratamento de códigos maliciosos e móveis.		X		
Maturidade Nível 2				
Existem ferramentas de controles para controlar códigos maliciosos.			X	
Existem treinamentos e ações de conscientização.		X		
A efetividade do processo está concentrada no colaborador		X		
Maturidade Nível 3				
Existem treinamentos e workshops periódicos visando conscientização sobre o tema				X
As ferramentas de controle possuem administração centralizada			X	
As aplicações que possuem códigos móveis emitem mensagens que auxiliam os colaboradores no seu uso seguro.				X
Maturidade Nível 4				
Existem indicadores de atuação das ferramentas de controle de códigos maliciosos e móveis.			X	
Os colaboradores são avaliados periodicamente sobre o uso das aplicações e seus riscos.				X
As ferramentas de controle bloqueiam os códigos desconhecidos.			X	
Maturidade Nível 5				
O comitê de segurança da informação utiliza os indicadores para a tomada de ações preventivas, corretivas e elaboração de projetos estratégicos.			X	
Os usuários possuem uma ferramenta de comunicação, onde solicitam a avaliação e liberação de códigos móveis relacionados as operações de negócio.				X
Os controles são automatizados e geram alertas em tempo real.			X	

DESCRIÇÃO DO PROCESSO

TEC04 – Cópias de Segurança

Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação. Convém que procedimentos de rotina sejam estabelecidos para implementar as políticas e estratégias definidas para a geração de cópias de segurança e possibilitar a geração das cópias de segurança dos dados e sua recuperação em um tempo aceitável.

OBJETIVOS DE CONTROLE

TEC04.1 – Cópias de segurança das informações

Convém que as cópias de segurança das informações e dos *softwares* sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

MODELO DE MATURIDADE

TEC04 – Cópias de Segurança

0 Não existente quando
A organização não possui qualquer tipo de preocupação com cópias de segurança, seja das informações ou dos softwares aplicativos utilizados.

1 Inicial/*Ad Hoc* quando
Algumas cópias de informações são realizadas pontualmente por colaboradores, sem com testes ou controles mais detalhados. Os softwares aplicativos são armazenados de maneira simples, sem controle de versão.

2 Repetível mas intuitivo quando
Os colaboradores estão mais sensibilizados em criar e manter cópias de segurança das informações de negócios, mas as ações não possuem procedimentos formais. As informações são armazenadas em um ambiente específico para este fim.

3 Definido quando
A organização assumiu a responsabilidade de criar e manter cópias de segurança das informações de negócio e estabeleceu procedimentos padrão para isso. Não existem indicadores de sucesso/falha das cópias e os procedimentos não são automatizados.

4 Gerenciado e Mensurável quando
A organização já possui um sistema automatizado para a realização das cópias de segurança. Testes periódicos são executados para avaliar a integridade e validade das cópias. Cópias de software aplicativos são mantidas em cofres, assim como suas respectivas licenças de uso. Os usuários são treinados para identificar falhas e alterações nas cópias de segurança.

5 Otimizado quando
O comitê de segurança da informação avalia regularmente os resultados e indicadores do sistema de cópias de segurança. As informações servem de base para toma de decisão estratégica e tática no que diz respeito a criar, manter e testar as cópias de segurança. Os procedimentos de retorno das cópias são eficiente e atendem aos requisitos de segurança requeridos pelo negócio.

QUESTIONÁRIO DE MATURIDADE

TEC04 – Cópias de Segurança

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Cópias de informações são realizadas por colaboradores, sem com testes ou controles mais detalhados.	X			
Os softwares aplicativos são armazenados de maneira simples, sem controle de versão.		X		
Maturidade Nível 2				
Os colaboradores estão sensibilizados em criar e manter cópias de segurança das informações de negócios.		X		
As informações são armazenadas em um ambiente específico para este fim.		X		
Os softwares aplicativos são armazenados de maneira simples, com controle de versão.		X		
Maturidade Nível 3				
A organização assumiu a responsabilidade de criar e manter cópias de segurança das informações de negócio e estabeleceu procedimentos padrão para isso.				X
Existem testes de sucesso/falha das cópias e os procedimentos não são automatizados			X	
As equipes são treinadas e conscientizadas sobre a guarda e geração e cópias de segurança.			X	
Maturidade Nível 4				
Existe um sistema automatizado para a realização das cópias de segurança				X
Testes periódicos são executados para avaliar a integridade das cópias				X
Cópias de software aplicativos são mantidas em cofres, assim como suas respectivas licenças de uso.			X	
Maturidade Nível 5				
O comitê de segurança da informação avalia regularmente os resultados e indicadores do sistema de cópias de segurança.				X
Os procedimentos de retorno das cópias são eficientes e atendem aos requisitos de segurança requeridos pelo negócio.				X

DESCRIÇÃO DO PROCESSO

TEC05 – Gerenciamento da Segurança em Redes

Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte. O gerenciamento seguro de redes, que pode ir além dos limites da organização, requer cuidadosas considerações relacionadas ao fluxo de dados, implicações legais, monitoramento e proteção.

OBJETIVOS DE CONTROLE

TEC05.1 – Controles de redes

Convém que as redes sejam adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito**.**

TEC05.2 – Segurança dos serviços de rede

Convém que as características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente ou terceirizados**.**

MODELO DE MATURIDADE

TEC05 – Gerenciamento da Segurança em Redes

0 Não existente quando
A organização não possui controles de segurança para a rede local e nem para os serviços de rede disponíveis.

1 Inicial/*Ad Hoc* quando
A rede já possui alguns controles de segurança, mas estão limitados a pontos específicos e são de operação da administração de redes da organização. Os serviços de rede não possuem monitoramento e não fazem parte de nenhum acordo de serviço.

2 Repetível mas intuitivo quando
Os controles de segurança de redes são aplicados pela gerência de redes de maneira de maneira organizada, mas não possuem a formalização de um processo. Alguns serviços de rede já possuem requisitos de disponibilidade e segurança, mas seu monitoramento é manual e pontual.

3 Definido quando
Os controles de segurança de redes foram definidos e formalmente informados. Eles possuem procedimentos operacionais claros e objetivos. O monitoramento ainda é pontual e não apresenta indicadores precisos. Os serviços de rede já possuem acordos definidos, mas não necessariamente aplicados.

4 Gerenciado e Mensurável quando
A gerência de rede monitora e gera indicadores relacionados a segurança de rede. As ferramentas de controles são automatizadas e geram informações para a tomada de decisão. Os acordos de nível de serviço são formais e controlados.

5 Otimizado quando
A segurança de redes passa por avaliações independentes periodicamente, utilizando ferramentas de avaliação e testes próprias. Os acordos de nível de serviços são monitorados e as eventuais não conformidades são analisadas e avaliadas.

QUESTIONÁRIO DE MATURIDADE

TEC05 – Gerenciamento da Segurança em Redes

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
A rede já possui controles de segurança e são de operação da administração de redes da organização.		X		
O monitoramento de rede é informal.	X			
Maturidade Nível 2				
Os controles de segurança de redes são aplicados pela gerência de redes de maneira de maneira organizada.		X		
Os serviços de rede possuem requisitos de disponibilidade e segurança.		X		
O monitoramento de rede é completo.		X		
Maturidade Nível 3				
Os controles de segurança de redes foram definidos e formalmente informados				X
Existem procedimentos operacionais claros e objetivos			X	
Os serviços de rede possuem acordos definidos			X	
O monitoramento de rede é completo.			X	
Maturidade Nível 4				
A gerência de rede monitora e gera indicadores relacionados a segurança de rede.				X
As ferramentas de controles são automatizadas.			X	
Os acordos de nível de serviço são formais e controlados.			X	
Maturidade Nível 5				
A segurança de redes passa por avaliações independentes periodicamente, utilizando ferramentas de avaliação e testes próprias.				X
Os acordos de nível de serviços são monitorados e as eventuais não conformidades são analisadas e avaliadas.			X	
O comitê de segurança da informação é informado sobre os indicadores e toma decisões preventivas/corretivas.			X	

DESCRIÇÃO DO PROCESSO

TEC06 – Manuseio de Mídias

Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades de negócio. Convém que as mídias sejam controladas e fisicamente protegidas.

OBJETIVOS DE CONTROLE

TEC06.1 – Gerenciamento de mídias removíveis
Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis.

TEC06.2 – Descarte de mídias
Convém que as mídias sejam descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.

TEC06.3 – Procedimentos para tratamento de informação
Convém que sejam estabelecidos procedimentos para o tratamento e o armazenamento de informações, para proteger tais informações contra a divulgação não autorizada ou uso indevido.

TEC06.4 – Segurança da documentação dos sistemas
Convém que a documentação dos sistemas seja protegida contra acessos não autorizados.

MODELO DE MATURIDADE

TEC06 – Manuseio de Mídias

0 Não existente quando
Não existe nenhum tipo de tratamento para as mídias na organização, seja para mídias móveis como para mídias de cópias de segurança. A organização não é sensível a divulgação de informações não autorizada.

1 Inicial/*Ad Hoc* quando
Já existe uma preocupação com a documentação dos sistemas de informação, mas de maneira pontual e dependente da sensibilidade dos colaboradores. A organização utiliza mídias removíveis sem controle específico e as mídias para descarte são destruídas de forma simples e não confiável. A organização já está se sensibilizando com o tratamento da informação e suas mídias de transporte.

2 Repetível mas intuitivo quando
Vários procedimentos para o descarte de mídias estão sendo aplicados, seguindo uma mesma lógica. O uso de mídias removíveis é controlado de maneira simples e mais focado no risco de infecção por vírus que por divulgação de informações. Já existem tutoriais de conscientização para o tratamento da informação.

3 Definido quando
A organização possui procedimentos formais de tratamento de mídias removíveis e todos os colaboradores são devidamente informados, conscientizados e treinados. O processo de descarte de mídias está definido e é aplicado por uma área responsável na organização. O tratamento da informação se tornou uma preocupação contínua na organização, sendo que as documentações de sistemas de informação são devidamente armazenadas e seu uso é controlado.

4 Gerenciado e Mensurável quando
A organização já possui indicadores do uso de mídias removíveis, quando autorizadas, assim como o descarte de mídias é controlado e gerenciado. Controles de acesso a documentos de sistemas são automatizados e exigem autorização explícita para acesso.

5 Otimizado quando
A maioria dos computadores da organização não suportam mídias móveis, e os que suportam são de acesso limitado e mediante autorização eletrônica. O descarte de mídias já é um processo automatizado, monitorado e controlado, onde são gerados indicadores de descarte e testes de informação residuais.

QUESTIONÁRIO DE MATURIDADE

TEC06 – Manuseio de Mídias

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
A organização utiliza mídias removíveis sem controle específico.		X		
As mídias para descarte são destruídas de forma simples e não confiável		X		
Maturidade Nível 2				
Procedimentos para o descarte de mídias foram criados e aplicados		X		
O uso de mídias removíveis é controlado de maneira simples e mais focado no risco de infecção por vírus.		X		
Existem tutoriais de conscientização para o tratamento da informação			X	
Maturidade Nível 3				
Existem procedimentos formais de tratamento de mídias removíveis e todos os colaboradores são devidamente informados, conscientizados e treinados.				X
O processo de descarte de mídias está definido e é aplicado por uma área responsável na organização.			X	
As documentações de sistemas de informação são devidamente armazenadas e seu uso é controlado.			X	
Maturidade Nível 4				
Existem indicadores do uso de mídias removíveis, quando autorizadas, assim como o descarte de mídias é controlado e gerenciado.				X
Controles de acesso a documentos de sistemas são automatizados e exigem autorização explícita para acesso.			X	
Maturidade Nível 5				
Os equipamentos da organização não suportam mídias móveis, e os que suportam são de acesso limitado e mediante autorização eletrônica.				X
O descarte de mídias já é um processo automatizado, monitorado e controlado.			X	

DESCRIÇÃO DO PROCESSO

TEC07 – Serviços de Comércio Eletrônico

Garantir a segurança de serviços de comércio eletrônico e sua utilização segura. Convém que as implicações de segurança da informação associadas com o uso de serviços de comércio eletrônico, incluindo transações on-line e os requisitos de controle, sejam consideradas. Convém que a integridade e a disponibilidade da informação publicada eletronicamente por sistemas publicamente disponíveis sejam também consideradas.

OBJETIVOS DE CONTROLE

TEC07.1 – Comércio eletrônico

Convém que as informações envolvidas em comércio eletrônico transitando sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas**.**

TEC07.2 – Transações *on-line*

Convém que informações envolvidas em transações on-line sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada**.**

TEC07.3 – Informações publicamente disponíveis

Convém que a integridade das informações disponibilizadas em sistemas publicamente acessíveis seja protegida para prevenir modificações não autorizadas**.**

MODELO DE MATURIDADE

TEC07 – Serviços de Comércio Eletrônico

0 Não existente quando
A organização não possui qualquer iniciativa de comércio eletrônico, suas transações on-line são baseadas em controles externos e as informações publicamente disponíveis não são monitoradas.

1 Inicial/*Ad Hoc* quando
As iniciativas de comércio eletrônico são poucas e limitadas a emissão e visualização de pedidos. As transações on-line são executadas com fornecedores que possuem sistemas de segurança aprimorados e internamente não requerem ações da organização. As informações públicas são controladas de maneira simples, ocasional e com grande dependência dos colaboradores.

2 Repetível mas intuitivo quando
A organização estabeleceu procedimentos para as iniciativas de comércio eletrônico, tanto do ponto de vista de cliente como do ponto de vista de fornecedor. Estes procedimentos são aplicados sob a responsabilidade individual de cada colaborador. Existem rotinas para preparação e tratamento de informações publicamente disponíveis, buscando organizá-las e proteger a imagem da organização.

3 Definido quando
Procedimentos de uso e aplicação de comércio eletrônico foram padronizados, documentados e comunicados através de treinamento. Os colaboradores foram conscientizados dos riscos e ameaças existentes e das formas de segurança disponíveis. Todas as transações on-line executadas seguem padrões r requisitos mínimos de segurança estabelecidos pelo comitê de segurança da informação. A publicação de informações é controlada e deve seguir o processo definido para este fim.

4 Gerenciado e Mensurável quando
O comitê de segurança da informação já recebe indicadores de desempenho e de segurança das transações de comércio eletrônico que agiliza a análise de riscos e a definição de novas arquiteturas de segurança. A organização implementou um sistema automatizado para a publicação de informações disponíveis com base nos conceitos de gerenciamento de conteúdo.

5 Otimizado quando
Os sistemas de comércio eletrônico seguem as melhores práticas internacionais e são monitorados e gerenciados com eficiência. Os indicadores são automatizados e alertas eletrônicos são emitidos em caso de detecção de não conformidades. Os sistemas de gerenciamento de conteúdo são integrados com o perfil dos colaboradores e totalmente automatizados.

QUESTIONÁRIO DE MATURIDADE

TEC07 – Serviços de Comércio Eletrônico

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
As iniciativas de comércio eletrônico são poucas e limitadas a emissão e visualização de pedidos.	X			
As transações on-line são executadas com fornecedores que possuem sistemas de segurança aprimorados.		X		
As informações públicas são controladas de maneira simples.	X			
Maturidade Nível 2				
A organização possui procedimentos para comércio eletrônico, tanto do ponto de vista de cliente como do ponto de vista de fornecedor.		X		
Existem rotinas para preparação e tratamento de informações publicamente disponíveis.			X	
Existem controles para organizar e proteger a imagem da organização		X		
Maturidade Nível 3				
Procedimentos de uso e aplicação de comércio eletrônico foram padronizados, documentados e comunicados através de treinamento.				X
Os colaboradores foram conscientizados dos riscos e ameaças existentes e das formas de segurança disponíveis.				X
Todas as transações on-line seguem padrões e requisitos mínimos de segurança estabelecidos pelo comitê de segurança da informação.			X	
A publicação de informações é controlada e deve seguir o processo definido.				X
Maturidade Nível 4				
O comitê de segurança da informação já recebe indicadores de desempenho e de segurança das transações de comércio eletrônico.			X	
Existe a análise de riscos e a definição de novas arquiteturas de segurança.			X	
Existe um sistema automatizado para a publicação de informações.				X
Maturidade Nível 5				
Os indicadores são automatizados e alertas eletrônicos são emitidos em caso de detecção de não conformidades				X
Os sistemas de gerenciamento de conteúdo são integrados com o perfil dos colaboradores e totalmente automatizados.			X	

DESCRIÇÃO DO PROCESSO

TEC08 – Gerenciamento de Acesso do Usuário

Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação. Convém que procedimentos formais sejam implementados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços.

OBJETIVOS DE CONTROLE

TEC08.1 – Registro de usuários

Convém que exista um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.

TEC08.2 – Gerenciamento de privilégios

Convém que a concessão e uso de privilégios sejam restritos e controlados.

TEC08.3 – Gerenciamento de senha do usuário

Convém que a concessão de senhas seja controlada através de um processo de gerenciamento formal.

TEC08.4 – Análise crítica dos direitos de acesso de usuário

Convém que o gestor conduza a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de processo formal.

MODELO DE MATURIDADE

TEC08 – Gerenciamento de Acesso do Usuário

0 Não existente quando
A organização não possui qualquer tipo de controle sobre os registros de usuários e seus privilégios em sistemas. As senhas ficam a critério dos usuários e não há análise crítica sobre estas questões.

1 Inicial/*Ad Hoc* quando
Alguns controles mínimos sobre a criação de usuários foram criados, mas sob responsabilidade de aplicação dos colaboradores. Os privilégios são fornecidos com base na solicitação inicial de criação e não são monitorados. Os usuários possuem um controle de senha mínimo, com base apenas no tempo de vida da senha.

2 Repetível mas intuitivo quando
Os procedimentos de registro de usuários evoluíram para um patamar onde são seguidas as mesmas rotinas. O gerenciamento dos privilégios ainda é com base nas solicitações, mas são alterados mediante pedidos formais. Análises críticas em pontos mais sensíveis são aplicadas em períodos não regulares.

3 Definido quando
A organização definiu procedimentos padrão para o registro de usuários e o gerenciamento de seus privilégios. Os procedimentos são manuais e foram comunicados e treinados soa usuários pertinentes. Foi criada uma política para a geração de senhas e os colaboradores foram sensibilizados a respeito disso.

4 Gerenciado e Mensurável quando
O processo de registro de usuários e geração de senhas e privilégios é monitorado e passa por análises críticas internas. A organização implantou um sistema de gerenciamento de identidade a fim de automatizar as atividades.

5 Otimizado quando
O gerenciamento de identidade é integrado com o departamento de recursos humanos e toda e qualquer alteração de perfil do usuário é registrada, monitorada e autorizada na organização. Indicadores fornecem informações para o comitê de segurança da informação, que associados aos resultados das análises críticas independentes, apoiam a toma de decisão estratégica em segurança da informação.

QUESTIONÁRIO DE MATURIDADE

TEC08 – Gerenciamento de Acesso do Usuário

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem controles mínimos sobre a criação de usuários, mas sob responsabilidade de aplicação dos colaboradores.	X			
Os privilégios são fornecidos com base na solicitação inicial de criação.		X		
Os usuários possuem um controle do tempo de vida da senha		X		
Maturidade Nível 2				
Existem procedimentos centralizados de registro de usuários		X		
O gerenciamento dos privilégios ainda é com base nas solicitações, mas são alterados mediante pedidos formais.		X		
Maturidade Nível 3				
Existem procedimentos padrão para o registro de usuários e o gerenciamento de seus privilégios.			X	
Os procedimentos são manuais e foram comunicados e treinados soa usuários pertinentes.				X
Existe uma política para a geração de senhas e os colaboradores foram sensibilizados a respeito disso.				X
Maturidade Nível 4				
O processo de registro de usuários e geração de senhas e privilégios é monitorado e passa por análises críticas internas.				X
Existe um sistema de gerenciamento de identidade a fim de automatizar as atividades.				X
Maturidade Nível 5				
O gerenciamento de identidade é integrado com o RH e toda alteração de perfil do usuário é registrada, monitorada e autorizada.				X
Indicadores fornecem informações para o comitê de segurança da informação.			X	
Os procedimentos e políticas são auditados periodicamente.			X	

DESCRIÇÃO DO PROCESSO

TEC09 – Controle de Acesso a Rede

Prevenir acesso não autorizado aos serviços de rede. Convém que o acesso aos serviços de rede internos e externos seja controlado, assim como convém que os usuários com acesso às redes e aos serviços de rede não comprometam a segurança desses serviços.

OBJETIVOS DE CONTROLE

TEC09.1 – Política de uso dos serviços de rede

Convém que usuários somente recebam acesso para os serviços que tenham sido especificamente autorizados a usar.

TEC09.2 – Autenticação para conexão externa do usuário

Convém que métodos apropriados de autenticações sejam usados para controlar acesso de usuários remotos.

TEC09.3 – Identificação de equipamentos em redes

Convém que sejam consideradas as identificações automáticas de equipamentos com um meio de autenticar conexões vindas de localizaçãoes e equipamentos específicos.

TEC09.4 – Proteção de portas de configuração e diagnóstico remotos

Convém que sejam controlados os acessos físico e lógico a portas de diagnóstico e configuração.

TEC09.5 – Segregação de redes

Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.

TEC09.6 – Controle de conexão de rede

Para redes compartilhadas, especialmente essas que se estendem pelos limites da organização, convém que a capacidade dos usuários para conectar-se à rede seja restrita, alinhada com a política de controle de acesso e os requisitos das aplicações do negócio.

TEC09.7 – Controle de roteamento de redes

Convém que seja implementado controle de roteamento na rede, para assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negócio.

MODELO DE MATURIDADE

TEC09 – Controle de Acesso a Rede

0 Não existente quando
A organização não possui qualquer tipo de política de uso dos serviços de rede, assim como qualquer tipo de controle para acesso e conexão a rede e serviços de rede.

1 Inicial/*Ad Hoc* quando
Alguns serviços de rede já possuem procedimentos próprios para acesso, mas não fazem parte de uma política estruturada. A rede não é segregada e os equipamentos ainda não possuem proteção em suas portas de manutenção, suporte e diagnóstico, mas eles são identificados seguindo um padrão definido.

2 Repetível mas intuitivo quando
Já existem vários procedimentos de controle de acesso a rede, assim como usuários por conexão remota são identificados e autenticados. A identificação dos equipamentos em redes é padronizada e suas portas de configuração e diagnóstico são protegidas. Uma iniciativa de segregação de redes já existe, mas ainda não é efetiva e é dependente dos colaboradores. Ainda não existe uma política de acesso a rede, mas o conjunto de procedimento já compõe um modelo para esta política.

3 Definido quando
Uma política de acesso a rede é definida, comunicada e reconhecida pelos usuários. A autenticação para utilizar os recursos de rede é obrigatória, mas não é monitorada. A segregação de redes é aplicada, mas não monitorada ou gerenciada. Não existem indicadores de gerenciamento. Os procedimentos de identificação dos equipamentos e as rotinas de proteção física e lógica das portas de configuração e diagnóstico é amplamente treinada pelos colaboradores pertinentes.

4 Gerenciado e Mensurável quando
A organização já possui sistemas automatizados para autenticar usuários e monitora o acesso as redes e serviços, Indicadores de desempenho e acesso são gerados, provendo informações de capacidade e segurança da informação. A segregação de redes é efetiva e controlada. A organização possui um inventário automático dos equipamentos de rede e suas configurações. A equipe de suporte gerencia o acesso aos equipamentos de maneira centralizada e monitorada.

5 Otimizado quando
O comitê de segurança da informação monitora as ações de acesso a rede através de relatórios de testes de penetração e dos indicadores dos sistemas automatizados. Análises críticas independentes são realizadas periodicamente visando identificar não conformidades nos controles e avaliar a sua efetividade em relação a política de acesso a rede.

QUESTIONÁRIO DE MATURIDADE

TEC09 – Controle de Acesso a Rede

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Os serviços de rede já possuem procedimentos próprios para acesso.	X			
A rede possui segregação e os equipamentos possuem proteção em suas portas de manutenção, suporte e diagnóstico.		X		
Maturidade Nível 2				
Existem procedimentos de controle de acesso a rede, assim como usuários por conexão remota são identificados e autenticados			X	
A identificação dos equipamentos em redes é padronizada e suas portas de configuração e diagnóstico são protegidas.		X		
Existe um conjunto de procedimentos que caracterizam uma política de acesso.		X		
Maturidade Nível 3				
A política de acesso a rede é definida, comunicada e reconhecida pelos usuários				X
A segregação de redes é aplicada por completo.			X	
A identificação dos equipamentos em redes é padronizada e suas portas de configuração e diagnóstico são protegidas é amplamente treinada pelos colaboradores pertinentes			X	
Maturidade Nível 4				
Existem sistemas automatizados para autenticar usuários e monitora o acesso as redes e serviços.			X	
Indicadores de desempenho e acesso são gerados, provendo informações de capacidade e segurança da informação.			X	
A segregação de redes é efetiva e controlada			X	
A equipe de suporte gerencia o acesso aos equipamentos de maneira centralizada e monitorada.				X
Maturidade Nível 5				
O comitê de segurança da informação monitora as ações de acesso a rede. Existem testes de penetração e os indicadores são automatizados				X
Análises críticas independentes são realizadas periodicamente.			X	

DESCRIÇÃO DO PROCESSO

TEC10 – Controle de Acesso ao Sistema Operacional

Prevenir acesso não autorizado aos sistemas operacionais. Convém que recursos de segurança da informação sejam usados para restringir o acesso aos sistemas operacionais para usuários autorizados.

OBJETIVOS DE CONTROLE

TEC10.1 – Procedimentos seguros de entrada no sistema (log-on)
Convém que o acesso aos sistemas operacionais seja controlado por um procedimento seguro de entrada no sistema (*log-on*).

TEC10.2 – Identificação e autenticação de usuário
Convém que todos os usuários tenham um identificador único (ID de usuário) para uso pessoal e exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário.

TEC10.3 – Sistema de gerenciamento de senha
Convém que sistemas de gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.

TEC10.4 – Uso de utilitários de sistema
Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado.

TEC10.5 – Limite de tempo de sessão
Convém que sessões inativas sejam encerradas após um período definido de inatividade.

TEC10.6 – Limitação de horário de conexão
Convém que restrições nos horários de conexões sejam utilizadas para proporcionar segurança adicional para aplicações de alto risco.

MODELO DE MATURIDADE

TEC10 – Controle de Acesso ao Sistema Operacional

0 Não existente quando
A organização não possui qualquer tipo de controle para o acesso aos sistemas operacionais, sendo que os usuários utilizam identificações genéricas e senhas compartilhadas.

1 Inicial/*Ad Hoc* quando
Alguns sistemas operacionais já exigem identificação única e senhas para acesso, mas ainda de maneira limitada e sem um gerenciamento de identidade adequado. A criação das senhas é de responsabilidade dos colaboradores, que podem acessar a qualquer tempo os sistemas.

2 Repetível mas intuitivo quando
A organização já possui procedimentos de acesso aos sistemas mais formalizados, onde cada usuário possui sua própria identificação. Existem recomendações para que a geração de senhas seja mais segura, mas não existe um sistema que avalie e teste as senhas dos colaboradores. Algumas aplicações possuem controle de tempo de inatividade de sessão, mas não limita o horário da conexão.

3 Definido quando
Os colaboradores possuem um acesso seguro ao sistema operacional e este procedimento é definido, comunicado e treinado. O sistema de autenticação é simples, mas eficiente, não havendo duas autenticações iguais. As senhas seguem um padrão formalizado pela organização, controlado pelo sistema de autenticação. Horários de acesso aos sistemaa são definidos, mas não são monitorados.

4 Gerenciado e Mensurável quando
A organização integrou o sistema de acesso ao sistema com o gerenciamento de identidade, onde é gerenciada a senha e a autenticação dos colaboradores. O sistema de gerenciamento de identidade é limitado ao procedimento de entrado no sistema (log-on). Já existem alguns indicadores de desempenho e de integridade das políticas de segurança de senha e de tentativas de acesso fora de horário.

5 Otimizado quando
O sistema de gerenciamento de identidade controla todo acesso ao sistema operacional e as aplicações de maneira automatizada. Existem controles específicos para sessões inativas e para os horários de conexão. Análises independentes externas são realizadas periodicamente a fim de validar as políticas e a eficácia dos controles.

QUESTIONÁRIO DE MATURIDADE

TEC10 – Controle de Acesso ao Sistema Operacional

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Os sistemas operacionais já exigem identificação única e senhas para acesso		X		
A criação das senhas é de responsabilidade dos colaboradores	X			
Maturidade Nível 2				
Existem procedimentos de acesso aos sistemas mais formalizados, onde cada usuário possui sua própria identificação.			X	
Existem recomendações para que a geração de senhas seja mais segura.		X		
As aplicações possuem controle de tempo de inatividade de sessão.		X		
Maturidade Nível 3				
Os colaboradores possuem um acesso seguro ao sistema operacional e este procedimento é definido, comunicado e treinado.				X
O sistema de autenticação é simples e rebusto.			X	
As senhas seguem um padrão formalizado pela organização, controlado pelo sistema de autenticação.			X	
Horários de acesso aos sistemas são definidos e controlados.			X	
Maturidade Nível 4				
O sistema de acesso ao sistema operacional é integrado com o gerenciamento de identidade.			X	
O gerenciamento de identidade gerencia a senha e a autenticação dos colaboradores.				X
Existem indicadores de desempenho e de integridade das políticas de segurança de senha.			X	
Existem indicadores acesso fora de horário e bloqueado.			X	
Maturidade Nível 5				
O sistema de gerenciamento de identidade controla todo acesso ao sistema operacional e as aplicações de maneira automatizada			X	
Existem controles para sessões inativas e para os horários de conexão.				X
Análises independentes externas são realizadas periodicamente a fim de validar as políticas e a eficácia dos controles.			X	

DESCRIÇÃO DO PROCESSO

TEC11 – Controle de Aceso a Aplicação e a Informação

Prevenir acesso não autorizado à informação contida nos sistemas de aplicação. Convém que os recursos de segurança da informação sejam utilizados para restringir o acesso aos sistemas de aplicação.

OBJETIVOS DE CONTROLE

TEC11.1 – Restrição de acesso à informação

Convém que o acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte seja restrito de acordo com o definido na política de controle de acesso**.**

TEC11.2 – Isolamento de sistemas sensíveis

Convém que sistemas sensíveis tenham um ambiente computacional dedicado (isolado)**.**

MODELO DE MATURIDADE

TEC11 – Controle de Acesso a Aplicação e a Informação

0 Não existente quando
Não existem definidas nenhuma restrição ou controle de acesso às informações ou às funções dos sistemas de aplicações da organização.

1 Inicial/*Ad Hoc* quando
Foram definidas algumas restrições de acesso à informação, mas de maneira simples e superficial. Os principais sistemas da organização e seus dados sensíveis compartilham o mesmo ambiente computacional dos demais serviços de rede, com poucos controles de acesso eficientes.

2 Repetível mas intuitivo quando
A organização se preocupa com o acesso a informação e estabeleceu alguns procedimentos mais detalhados relacionados a restringir acesso. Alguns sistemas já possuem controle de acesso. Iniciativas de se isolar serviços já são identificadas, mas ainda de maneira rudimentar.

3 Definido quando
Todos os sistemas e aplicações são alocados em uma área isolada e segregada, aumentando assim a restrição de acesso aos mesmos. Procedimentos foram padronizados, documentados e comunicados através de treinamento. Existe monitoramento pontual sobre algumas aplicações. A informação é encarada como ativo da organização e procedimentos e restrições de acesso foram definidos.

4 Gerenciado e Mensurável quando
A segurança da informação e o acesso a informação são iniciativas organizadas, definidas e gerenciadas pela organização. Os sistemas foram segregados e seu ambiente é monitorado e gerenciado. Indicadores precisos relacionados as restrições e tentativas de acessos não autorizados são gerados.

5 Otimizado quando
O controle de acesso e as restrições relacionadas a ele são gerenciados por aplicações automatizadas e integradas ao gerenciamento de identidade. O ambiente das aplicações é segregado e possui sistemas automatizados de prevenção e detecção de intrusão. Alertas são gerados automaticamente e incidentes são reportados ao comitê de segurança da informação.

QUESTIONÁRIO DE MATURIDADE

TEC11 – Controle de Acesso a Aplicação e a Informação

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem restrições de acesso à informação.	X			
Os principais sistemas da organização e seus dados sensíveis compartilham o mesmo ambiente computacional dos demais serviços de rede.		X		
Maturidade Nível 2				
O acesso a informação possui procedimentos de restringir o acesso indevido			X	
Os sistemas já possuem controle de acesso		X		
A segregação de serviços é utilizada.		X		
Maturidade Nível 3				
Os sistemas e aplicações são alocados em uma área isolada e segregada, aumentando assim a restrição de acesso aos mesmos.				X
Procedimentos foram padronizados, documentados e comunicados através de treinamento.			X	
Existe monitoramento sobre as aplicações		X		
A informação é encarada como ativo da organização.				X
Maturidade Nível 4				
A segurança da informação e o acesso a informação são iniciativas organizadas, definidas e gerenciadas.			X	
Os sistemas foram segregados e seu ambiente é monitorado e gerenciado.			X	
Indicadores precisos relacionados as restrições e tentativas de acessos não autorizados são gerados.			X	
Maturidade Nível 5				
O controle de acesso e as restrições relacionadas a ele são gerenciados por aplicações automatizadas.			X	
A integração dos controles com o gerenciamento de identidade é total.				X
O ambiente das aplicações é segregado e possui sistemas automatizados de prevenção e detecção de intrusão.			X	
Alertas são gerados automaticamente e incidentes são reportados ao comitê de segurança da informação			X	

DESCRIÇÃO DO PROCESSO

TEC12 – Computação Móvel e Trabalho Remoto

Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto. Convém que a proteção requerida seja proporcional com o risco desta forma específica de trabalho.

OBJETIVOS DE CONTROLE

TEC12.1 – Computação e comunicação móvel

Convém que uma política formal seja estabelecida e que medidas de segurança apropriadas sejam adotadas para a proteção contra riscos do uso de recursos de computação e comunicação móveis.

TEC12.2 – Trabalho remoto

Convém que uma política, planos operacionais e procedimentos sejam desenvolvidos e implementados para atividades de trabalho remoto.

MODELO DE MATURIDADE

TEC12 – Computação Móvel e Trabalho Remoto

0 Não existente quando
A organização não demonstra preocupação ou está sensibilizada com os riscos inerentes ao uso da computação móveis ou acessos via conexões remotas.

1 Inicial/*Ad Hoc* quando
Já existem alguns controles relacionados ao trabalho remoto, principalmente no que diz respeito a autenticação dos usuários, mas estes controles ainda são manuais e rudimentares. A comunicação móvel é controlada através de algoritmos comuns de criptografia, mas visando apenas proteger a rede de acessos indevidos e não com foco na proteção da informação.

2 Repetível mas intuitivo quando
Procedimentos mais detalhados e complexos para o trabalho remoto foram desenvolvidos, mas os controles são sensíveis às habilidades dos colaboradores e podem sofrer alterações não autorizadas. O trabalho com dispositivos móveis pelos colaboradores são limitados a apenas alguns recursos, mas não existe monitoramento ou controle mais detalhado.

3 Definido quando
Os procedimentos de trabalho remoto foram formalmente definidos, comunicados e treinados. Somente colaboradores autorizados acessam aplicações específicas. O monitoramento é limitado a autenticação dos usuários. A computação móvel é segregada dos demais ambientes e procedimentos de conexão são definidos e controlados.

4 Gerenciado e Mensurável quando
A organização gerencia e monitora todos os acessos remotos e possui ferramentas de prevenção e detecção de invasões. A autenticação dos usuários remotos é integrada com o gerenciamento de identidade da organização. A computação móvel é monitorada e também possui ferramentas de prevenção e detecção de invasão. Existem indicadores de acesso remoto (origem-destino-usuário).

5 Otimizado quando
Os acessos remotos e móveis são controlados pelo gerenciamento de identidade, limitando horários de conexão e finalizando sessões inativas. Indicadores de eventos de não conformidade são gerados e processados para análises do comitê de segurança da informação. Testes de penetração e análises independentes são realizadas periodicamente.

QUESTIONÁRIO DE MATURIDADE

TEC12 – Computação Móvel e Trabalho Remoto

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem alguns controles relacionados ao trabalho remoto, principalmente no que diz respeito a autenticação dos usuários.		X		
A comunicação móvel é controlada através de algoritmos de criptografia.	X			
Maturidade Nível 2				
O trabalho com dispositivos móveis são limitados a alguns recursos.		X		
A comunicação móvel é controlada através de algoritmos de criptografia.			X	
Existem alguns controles relacionados ao trabalho remoto, principalmente no que diz respeito a autenticação dos usuários.			X	
Maturidade Nível 3				
Os procedimentos de trabalho remoto são formalmente definidos, comunicados e treinados.				X
Somente colaboradores autorizados acessam aplicações específicas.			X	
O monitoramento é limitado a autenticação dos usuários.				X
A computação móvel é segregada dos demais ambientes e procedimentos de conexão são definidos e controlados.			X	
Maturidade Nível 4				
Existe gerenciamento e monitoração dos acessos remotos, assim como ferramentas de prevenção e detecção de invasões.			X	
A autenticação dos usuários remotos é integrada com o gerenciamento de identidade da organização				X
A computação móvel é monitorada e também possui ferramentas de prevenção e detecção de invasão.			X	
Maturidade Nível 5				
Os acessos remotos e móveis são controlados pelo gerenciamento de identidade, limitando horários de conexão e finalizando sessões inativas.				X
Indicadores de eventos de não conformidade são gerados e processados para análises do comitê de segurança da informação.			X	
Testes de penetração e análises independentes são realizadas periodicamente.			X	

DESCRIÇÃO DO PROCESSO

TEC13 – Processamento Correto nas Aplicações

Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mal uso de informações em aplicações. Convém que controles apropriados sejam incorporados no projeto das aplicações, inclusive aquelas desenvolvidas pelos usuários, para assegurar o processamento correto. Convém que esses controles incluam a validação dos dados de entrada, do processamento interno e dos dados de saída.

OBJETIVOS DE CONTROLE

TEC13.1 – Validação dos dados de entrada

Convém que os dados de entrada das aplicações sejam validados para garantir que são corretos e apropriados.

TEC13.2 – Controle do processamento interno

Convém que sejam incorporadas, nas aplicações, checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas.

TEC13.3 – Integridade de mensagens

Convém que requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações sejam identificados e os controles apropriados sejam identificados e implementados.

TEC13.4 – Validação de dados de saída

Convém que os dados de saída das aplicações sejam validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.

MODELO DE MATURIDADE

TEC13 – Processamento Correto nas Aplicações

0 Não existente quando
A organização não controla qualitativamente as informações processadas nos sistemas de informação através de controles específicos, assim como não determina a necessidade de análise das informações inseridas ou obtidas dos sistemas.

1 Inicial/*Ad Hoc* quando
A organização possui preocupação com a entrada de dados nos sistemas de informação, mas fica a critério de cada gestor de sistema o controle destes dados. Os sistemas passam por testes de QA (*quality assurance*) quando solicitados pelas áreas usuárias.

2 Repetível mas intuitivo quando
Os dados processados nas aplicações são periodicamente avaliados, mas os critérios de avaliação variam de acordo com o gestor responsável. Alguns sistemas possuem controles mais específicos para prevenir a modificação de dados não autorizada. As equipes de QA buscam aplicar os mesmos critérios de avaliação qualitativa das informações processadas no sistemas, assim como buscam a padronização dos dados de entrada.

3 Definido quando
Existe uma equipe de QA (*quality assurance*) responsável pelo controle das aplicações e as informações por elas geradas. Esta equipe definiu processos para avaliar e controlar tanto a entrada como a saída de informações dos sistemas de informação. Além disso, existem controles intermediários para a avaliar as informações durante seu ciclo de processamento. Os processos são executados de maneira manual, sem apoio de ferramentas. Os indicadores são claros, mas exigem grande esforço para sua geração.

4 Gerenciado e Mensurável quando
Os processos de controle das informações e QA são gerenciados de maneira mais eficiente, fazendo parte da visão e estratégia corporativa. Os indicadores são controlados e reportados periodicamente, fazendo parte das metas das equipes de QA. Já existem controles automatizados aplicados nas interfaces dos sistemas.

5 Otimizado quando
Os processos foram refinados a um nível onde a aderência a normas e boas práticas é muito grande, assim como são aplicadas soluções de melhoria contínua como PDCA. Existem automatizações de alto nível que monitoram em tempo real as aplicações e geram alertas específicos quando desvios são identificados. A gerência da organização utiliza os indicadores com alto grau de confiança para a tomada de decisões.

QUESTIONÁRIO DE MATURIDADE

TEC13 – Processamento Correto nas Aplicações

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Os sistemas passam por testes de QA (*quality assurance*) quando solicitados pelas áreas usuárias		X		
A entrada de dados nos sistemas de informação possui controle de dados	X			
Maturidade Nível 2				
Os dados processados nas aplicações são periodicamente avaliados		X		
Os sistemas passam por testes de QA (*quality assurance*) quando solicitados pelas áreas usuárias			X	
Existem controles para prevenir a modificação de dados não autorizada		X		
Maturidade Nível 3				
Existe uma equipe de QA (*quality assurance*) responsável pelo controle das aplicações e as informações por elas geradas.			X	
Existem processos para avaliar e controlar tanto a entrada como a saída de informações dos sistemas de informação			X	
Existem controles intermediários para a avaliar as informações durante seu ciclo de processamento			X	
Maturidade Nível 4				
Os processos de controle das informações e QA são gerenciados de maneira mais eficiente, fazendo parte da visão e estratégia corporativa				X
Os indicadores são controlados e reportados periodicamente, fazendo parte das metas das equipes de QA.				X
Existem controles automatizados aplicados nas interfaces dos sistemas			X	
Maturidade Nível 5				
Existem automatizações de alto nível que monitoram em tempo real as aplicações e geram alertas específicos quando desvios são identificados.			X	
O comitê de segurança da informação gerencia os indicadores do processo de maneira proativa.			X	

DESCRIÇÃO DO PROCESSO

TEC14 – Controles Criptográficos

Proteger a confidencialidade, a autenticidade e a integridade das informações por meios criptográficos. Convém que uma política seja desenvolvida para o uso de controles criptográficos, assim como o gerenciamento de chaves seja implementado para apoiar o uso de técnicas criptográficas.

OBJETIVOS DE CONTROLE

TEC14.1 – Política para o uso de controles criptográficos

Convém que seja desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação. Esta política deve estar alinhada com a política de Segurança da Informação da organização e também deve prever que o uso de controles criptográficos faça parte das análises de riscos de segurança da informação.

TEC14.2 – Gerenciamento de chaves

Convém que um processo de gerenciamento de chaves seja planejado e implantado para apoiar o uso de técnicas criptográficas pela organização. As chaves criptográficas precisam ser adequadamente protegidas contra modificação não autorizada, perda ou destruição.

MODELO DE MATURIDADE

TEC14 – Controles Criptográficos

0 Não existente quando
A organização não utiliza controles criptográficos, seja por falta de conhecimento, cultura ou mesmo interesse. Estes controles não são vistos como necessários.

1 Inicial/*Ad Hoc* quando
A organização identificou a necessidade de utilizar controles criptográficos, mas de maneira muito pontual e principalmente a critério de cada indivíduo. As iniciativas são muito mais de caráter pessoal que institucional.

2 Repetível mas intuitivo quando
A criptografia teve seu uso aumentado dentro da organização, que reconheceu a necessidade de padronizar as iniciativas. Os usuários utilizam os controles criptográficos de maneira semelhante, mas não existe uma preocupação em relação ao gerenciamento das chaves criptográficas. O armazenamento das chaves é realizado por cada indivíduo que determina como fazê-lo.

3 Definido quando
A organização definiu um processo específico para a utilização de controles criptográficos. Junto com este processo, foi elaborada e publicada uma política de uso para os controles. Os colaboradores são aculturados da necessidade de segurança da informação e como os controles criptográficos podem auxiliar neste sentido. Os procedimentos foram padronizados, documentados e comunicados através de treinamento. A guarda das chaves é centralizada pela organização que fornece o apoio necessário e suficiente para o uso adequado de criptografia.

4 Gerenciado e Mensurável quando
A utilização de controles criptográficos é intensa, sendo base para muitas das aplicações da organização. Os usuários são treinados e reciclados com periodicidade e passam por avaliações sistêmicas. Foram gerados indicadores do uso dos controles e da aderência que os sistemas e procedimentos reais possuem com as normas e políticas de segurança da informação da organização. As chaves são gerenciadas de maneira manual, mas com eficiência suficiente para suportar as necessidades da organização. O uso dos controles é monitorado manualmente, sempre respeitando e observando a política definida.

5 Otimizado quando
A organização encara os controles criptográficos como uma forte ferramenta de segurança da informação, seu uso é incentivado e controlado de maneira consistente. Existem indicadores fortes relacionados ao uso de criptografia e como ela é gerenciada na organização. Os sistemas de informação e acessos em geral são baseados em criptografia conforme a política de uso da organização. Existe um monitoramento automático e geração de alertas e bloqueios relacionados aos canais criptografados.

QUESTIONÁRIO DE MATURIDADE

TEC14 – Controles Criptográficos

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existe o uso de controles criptográficos		X		
As iniciativas são muito mais de caráter pessoal que institucional	X			
Maturidade Nível 2				
Os usuários utilizam os controles criptográficos de maneira semelhante.			X	
O armazenamento das chaves é realizado por cada indivíduo.		X		
Maturidade Nível 3				
Existe um processo específico para a utilização de controles criptográficos e foi elaborada e publicada uma política de uso para os controles.				X
Os colaboradores são conscientizados da necessidade do uso de controles criptográficos			X	
Os procedimentos foram padronizados, documentados e comunicados através de treinamento.				X
A guarda das chaves é centralizada pela organização.			X	
Maturidade Nível 4				
A utilização de controles criptográficos é intensa.				X
Os usuários são treinados e reciclados com periodicidade e passam por avaliações sistêmicas.			X	
Existem indicadores do uso dos controles e da aderência que os sistemas e procedimentos possuem com as normas e políticas de segurança.			X	
Maturidade Nível 5				
A organização encara os controles criptográficos como uma forte ferramenta de segurança da informação.				X
Existem indicadores fortes relacionados ao uso de criptografia e como ela é gerenciada na organização.			X	
Existe um monitoramento automático e geração de alertas e bloqueios relacionados aos canais criptografados.			X	

DESCRIÇÃO DO PROCESSO

TEC15 – Segurança nos Arquivos de Sistema

Garantir a segurança de arquivos de sistema através do controle de acesso aos mesmos e aos programas de código fonte. Os controles também têm como objetivo evitar a exposição de dados sensíveis em ambientes de teste.

OBJETIVOS DE CONTROLE

TEC15.1 – Controle de software operacional

Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados, minimizando o risco de corrupção de sistemas operacionais, pirataria e mau uso.

TEC15.2 – Proteção dos dados para teste de sistema

Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados a fim de evitar a exposição de dados sensíveis a usuários não autorizados, ou mesmo a outras organizações, como prestadores de serviços.

TEC15.3 – Controle de acesso ao código fonte de programa

Convém que o acesso ao código fonte de programas seja restrito e controlado.

MODELO DE MATURIDADE

TEC15 – Segurança nos Arquivos de Sistema

0 Não existente quando
A organização n]ao reconhece a necessidade de controlar o acesso ao sistema operacional ou qualquer outro tipo de controle sobre software e informações.

1 Inicial/*Ad Hoc* quando
Existem alguns controles relacionados a instalação de softwares homologados, mas são caracterizados por apenas for ter suporte interno. As aplicações são testadas com cópias dos banco de dados de produção no ambiente de teste.

2 Repetível mas intuitivo quando
As iniciativas de controle abrangem quase todos os computadores da organização, mas os controles ainda são baseados na confiança no usuário. Os ambientes de testes são segregados, mas ainda utilizam cópias integrais das informações de produção. Os códigos fontes de aplicações, sistemas operacionais e aplicativos em gerais são armazenados de maneira conjunta.

3 Definido quando
A área de tecnologia da informação adotou procedimentos padronizados para a instalação de softwares e consegue, através de controles específicos, inibir a instalação de softwares não homologados. O ambiente de teste é mais segregado, com as informações de teste ainda sendo uma imagem integral do ambiente de produção. Existem controles definidos para a armazenagem de códigos fonte (tanto de aplicações como de sistemas operacionais).

4 Gerenciado e Mensurável quando
Os controles de detecção de softwares não homologados são aplicados, gerando alertas para a equipe de suporte e monitoração. Os usuários precisam solicitar formalmente a instalação de aplicações e outros softwares. O ambiente de teste utiliza informações previamente selecionadas para testes, a fim de proteger dados sensíveis. O gerenciamento do processo é reativo aos alertas.

5 Otimizado quando
O processo de instalação de softwares possui forte alinhamento com o Cumprimento de Requisições do ITIL. Existem indicadores consistentes sobre as solicitações de instalação de softwares. As equipes de teste realizam as atividades com informações adequadamente preparadas e que refletem o perfil das informações de produção. A guarda de códigos fontes é realizada em cofres específicos e seu controle e monitoramento é realizado através de chamados (Cumprimento de Requisições).

QUESTIONÁRIO DE MATURIDADE

TEC15 – Segurança nos Arquivos de Sistema

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem controles relacionados a instalação de softwares homologados		X		
As aplicações são testadas com cópias dos bancos de dados de produção no ambiente de teste		X		
Maturidade Nível 2				
Os controles abrangem os computadores da organização			X	
Os ambientes de testes são segregados, mas ainda utilizam cópias integrais das informações de produção.			X	
Os códigos fontes de aplicações, sistemas operacionais e aplicativos em gerais são armazenados de maneira conjunta.		X		
Maturidade Nível 3				
Existem procedimentos padronizados para a instalação de softwares para inibir a instalação de softwares não homologados				X
Os ambientes de testes são segregados, mas utilizam cópias integrais das informações de produção.				X
Existem controles definidos para a armazenagem de códigos fonte (tanto de aplicações como de sistemas operacionais)			X	
Maturidade Nível 4				
Os controles de detecção de softwares não homologados são aplicados, gerando alertas para a equipe de suporte e monitoração.				X
Os usuários solicitam formalmente a instalação de aplicações e softwares.				X
O ambiente de teste utiliza informações previamente selecionadas para testes, a fim de proteger dados sensíveis.			X	
O gerenciamento do processo é reativo aos alertas.			X	
Maturidade Nível 5				
O processo de instalação de softwares possui forte alinhamento com o Cumprimento de Requisições do ITIL.				X
Existem indicadores sobre as solicitações de instalação de softwares			X	
A guarda de códigos fontes é realizada em cofres específicos e seu controle e monitoramento é realizado através de chamados.			X	

DESCRIÇÃO DO PROCESSO

TEC16 – Segurança em Processos de Desenvolvimento e de Suporte

Manter a segurança de sistemas aplicativos e da informação, tanto em ambientes de projeto como em ambientes de suporte. Assegurar que as mudanças são liberadas e aplicadas corretamente.

OBJETIVOS DE CONTROLE

TEC16.1 – Procedimentos para controle de mudanças

Convém que a implementação de mudanças seja controlada utilizando procedimentos formais de controle de mudanças. Os controles de mudanças devem ser adequadamente documentados e auditados.

TEC16.2 – Análise crítica técnica das aplicações após mudanças no sistema operacional

Convém que aplicações críticas de negócios sejam analisadas criticamente e testadas quando sistemas operacionais são mudados, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.

TEC16.3 – Restrições sobre mudanças em pacotes de *software*

Convém que modificações em pacotes de *software* sejam desencorajadas e limitadas às mudanças necessárias e que todas as mudanças sejam estritamente controladas.

TEC16.4 – Vazamento de informações

Convém que oportunidades para vazamento de informações sejam prevenidas.

TEC16.5 – Desenvolvimento terceirizado de software

Convém que a organização supervisione e monitore o desenvolvimento terceirizado de software.

MODELO DE MATURIDADE

TEC16 – Segurança em Processos de Desenvolvimento e de Suporte

0 Não existente quando
Não existe um tratamento para as mudanças de software. A organização não desenvolve *software* e o suporte as aplicações são realizadas de maneira emergencial, sem documentação ou controle.

1 Inicial/*Ad Hoc* quando
A organização se preocupa em manter os sistemas operacionais atualizados, seguindo as orientações gerais dos seus fornecedores, sendo na maioria das vezes executadas as atualizações automáticas. O desenvolvimento de software existe e as mudanças são realizadas quando solicitadas. Não existem controles sobre as mudanças, nem documentação sobre as mesmas. A organização se preocupa com o vazamento de informações somente no que diz respeito a conscientização. Serviços de terceiros não são formalmente controlados.

2 Repetível mas intuitivo quando
As mudanças em sistemas operacionais seguem um padrão que é a maneira pela qual a tecnologia de informação realiza suas atividades, mas ainda depende muito de cada colaborador seguir os procedimentos. Foram aplicados formulários de solicitações de mudanças nos sistemas, a fim de documentar as mudanças. Terceiros são contratados para desenvolver aplicações e são controlados pelas equipes de desenvolvimento ou seus gestores, mas o controle se restringe ao uso de recursos (principalmente financeiros).

3 Definido quando
Existe um processo de desenvolvimento de software formalizado, com um controle sobre mudanças mais efetivo e restritivo. Já existe implantado o conceito de Requisições de Mudanças (*RFC - Request for Changes*). Os sistemas operacionais são atualizados conforme as necessidades e sempre com base em testes em ambientes específicos. A segurança das informações no desenvolvimento, tanto para equipes internas quanto para terceiros, é baseado em termos de não divulgação (*NDA – Not Disclosure Agreement*).

4 Gerenciado e Mensurável quando
As mudanças sofrem revisões pós-implementações que medem a aderência e efetividade das mudanças, assim como são medidos os incidentes relacionados a mudanças mal sucedidas. No ambiente de desenvolvimento são utilizadas apenas informações previamente preparadas, a fim evitar o vazamento de informações sensíveis. Os sistemas operacionais são monitorados e controlados de maneira proativa, gerando alertas sobre falhas e erros. Indicadores de mudanças foram implantados e constantemente avaliados.

5 Otimizado quando
Os processos foram refinados a um nível de boas práticas, tomando como base o ITIL (gerenciamento de mudanças). A segurança das informações de teste e homologação é baseada em dados devidamente preparados para este fim. As mudanças emergenciais precisam de aprovação e testes de vários níveis. A gerência possui uma visão consolidada sobre o desenvolvimento de software e seus impactos nas mudanças solicitadas.

QUESTIONÁRIO DE MATURIDADE

TEC16 – Segurança em Processos de Desenvolvimento e de Suporte

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
O desenvolvimento de software existe e as mudanças são realizadas quando solicitadas		X		
Serviços de terceiros não são formalmente controlados.		X		
Os sistemas operacionais são atualizados seguindo orientações dos seus fornecedores.		X		
Maturidade Nível 2				
As mudanças em sistemas operacionais seguem um padrão		X		
Existem formulários de solicitações de mudanças nos sistemas, a fim de documentar as mudanças.			X	
Serviços de terceiros não são formalmente controlados.			X	
Maturidade Nível 3				
Existe um processo de desenvolvimento de software formalizado, com um controle sobre mudanças mais efetivo e restritivo				X
Existe implantada a Requisição de Mudanças (*RFC - Request for Changes*)			X	
Os sistemas operacionais são atualizados conforme as necessidades e sempre com base em testes em ambientes específicos			X	
Colaboradores e terceiros assinam o termo de não divulgação (NDA)		X		
Maturidade Nível 4				
As mudanças sofrem revisões pós-implementações que medem a aderência e efetividade das mudanças			X	
São medidos os incidentes relacionados a mudanças mal sucedidas			X	
Indicadores de mudanças foram implantados e constantemente avaliados.				X
Maturidade Nível 5				
A segurança das informações de teste e homologação é baseada em dados devidamente preparados para este fim			X	
As mudanças emergenciais precisam de aprovação e testes de vários níveis.				X
Existe uma visão consolidada sobre o desenvolvimento de software e seus impactos nas mudanças solicitadas			X	

DESCRIÇÃO DO PROCESSO

TEC17 – Gestão de Vulnerabilidades Técnicas

Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas. Convém que a implementação da gestão de vulnerabilidades técnicas seja implementada de forma efetiva, sistemática e de forma repetível, com medições de confirmação da efetividade.

OBJETIVOS DE CONTROLE

TEC17.1 – Controle de vulnerabilidades técnicas

Convém que seja obtida informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a estas vulnerabilidades e tomadas às medidas apropriadas para lidar com os riscos associados.

MODELO DE MATURIDADE

TEC17 – Gestão de Vulnerabilidades Técnicas

0 Não existente quando
A organização não possui iniciativas relacionadas a gestão de vulnerabilidades técnicas dos sistemas de informação.

1 Inicial/*Ad Hoc* quando
A organização identificou a necessidade de tratar algumas vulnerabilidades devido a incidentes, mas este tratamento é baseado na percepção dos colaboradores responsáveis. Muitas vulnerabilidades existentes são tratadas e aceitas como bugs de sistemas.

2 Repetível mas intuitivo quando
As vulnerabilidades possuem um procedimento de tratamento definido, mas sua identificação ainda é pontual e depende da percepção dos colaboradores. Informativos dos fornecedores são consultados a fim de obter mais informações sobre erros, falhas e vulnerabilidades.

3 Definido quando
O procedimento de análise de vulnerabilidades é formal, as equipes seguem padrões de identificação e tratamento. A gestão de vulnerabilidades é incipiente e não existem indicadores consolidados. Treinamentos e workshops de conscientização são realizados buscando a criação da cultura em relação as vulnerabilidades.

4 Gerenciado e Mensurável quando
A gestão de vulnerabilidades é mais estruturada, indicadores periódicos são analisados e decisões de controles e remediação são tomadas com base neles. Os sistemas possuem tratamento de vulnerabilidades e sua identificação é apoiada pela percepção dos usuários finais.

5 Otimizado quando
O processo está bem definido e seguido. As equipes de desenvolvimento utilizam pacotes de análise de vulnerabilidades já durante a especificação e desenvolvimento de sistemas. A gestão é proativa, indicadores compõe o dashboard dos gerentes e as vulnerabilidades são avaliadas junto a outras iniciativas, como mudanças e incidentes. O monitoramento é baseado em ferramentas automatizadas (como IPS, IDS) e ações corretivas são avaliadas, aplicadas e documentadas.

QUESTIONÁRIO DE MATURIDADE

TEC17 – Gestão de Vulnerabilidades Técnicas

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Vulnerabilidades existentes são tratadas e aceitas como bugs de sistemas.		X		
Existem vulnerabilidades que geram incidentes.		X		
Maturidade Nível 2				
As vulnerabilidades possuem um procedimento de tratamento definido			X	
Informativos dos fornecedores são consultados a fim de obter mais informações sobre erros, falhas e vulnerabilidades.		X		
Existem vulnerabilidades que geram incidentes.			X	
Maturidade Nível 3				
O procedimento de análise de vulnerabilidades é formal, as equipes seguem padrões de identificação e tratamento				X
Treinamentos e workshops de conscientização são realizados buscando a criação da cultura em relação as vulnerabilidades.			X	
Maturidade Nível 4				
A gestão de vulnerabilidades é mais estruturada, indicadores periódicos são analisados.			X	
Os sistemas possuem tratamento de vulnerabilidades e sua identificação é apoiada pela percepção dos usuários finais				X
Maturidade Nível 5				
As equipes de desenvolvimento utilizam pacotes de análise de vulnerabilidades já durante a especificação e desenvolvimento de sistemas			X	
A gestão é proativa, indicadores compõe o dashboard dos gerentes e as vulnerabilidades são avaliadas junto a outras iniciativas, como mudanças e incidentes			X	
O monitoramento é baseado em ferramentas automatizadas (como IPS, IDS) e ações corretivas são avaliadas, aplicadas e documentadas				X

DESCRIÇÃO DO PROCESSO

GES01 – Notificação de Fragilidades e Eventos de Segurança da Informação

Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

OBJETIVOS DE CONTROLE

GES01.1 – Notificação de eventos de segurança da informação

Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível. Além disso, também é importante relatar os procedimentos de resposta aos incidentes e seu respectivo escalonamento.

GES01.2 – Notificando fragilidades de segurança da informação

Convém que os funcionários, fornecedores e terceiros de sistemas e serviços de informação sejam instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços.

MODELO DE MATURIDADE

GES01 – Notificação de Fragilidades e Eventos de Segurança da Informação

0 Não existente quando
A organização não se preocupa em comunicar os incidentes de segurança da informação, assim como os colaboradores não são preparados para identifica-los.

1 Inicial/*Ad Hoc* quando
Os eventos de segurança da informação são relatados como incidentes ou falhas de tecnologia da informação. A gestão da empresa não tem como diferenciar entre segurança de redes e segurança da informação. As iniciativas de conscientização dizem respeito somente a políticas de segurança simples.

2 Repetível mas intuitivo quando
Já existe uma diferenciação para classificar um incidente de segurança da informação, e com isso foram propostos certos tipos de notificações para a gerência da organização. Os usuários recebem instruções e orientações sobre os riscos e incidentes de segurança da informação. Os incidentes de segurança são tratados de maneira priorizada.

3 Definido quando
A política de segurança da informação orienta a organização no escalonamento e reporte de incidentes. Os colaboradores possuem um canal formal para notificar incidentes e vulnerabilidades. As equipes de resposta a incidentes são especificamente treinadas e possui acesso a gerência da organização. Os processos e procedimentos são definidos, mas sem automatizações ou medidas.

4 Gerenciado e Mensurável quando
São gerados indicadores de incidentes de segurança da informação e reportados a gerencia periodicamente. A monitoração sobre recursos críticos de TI são proativos. Os colaboradores recebem treinamento detalhado sobre a identificação e notificação de vulnerabilidades.

5 Otimizado quando
A tomada de decisão corporativa leva em consideração os históricos de incidentes de segurança da informação e acompanham o tema dentro do contexto de gerenciamento. As equipes possuem especialistas em assuntos específicos como RH, Redes, Suporte, Legislação e Auditoria. Os colaboradores possuem ferramentas automatizadas para relatar vulnerabilidades e outras ações que julguem de riscos para a organização.

QUESTIONÁRIO DE MATURIDADE

GES01 – Notificação de Fragilidades e Eventos de Segurança da Informação

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Os eventos de segurança da informação são relatados como incidentes ou falhas de tecnologia da informação.		X		
As iniciativas de conscientização dizem respeito somente a políticas de segurança simples.			X	
Segurança de redes é o mesmo conceito que segurança da informação.	X			
Maturidade Nível 2				
Os colaboradores sabem diferenciar entre segurança de redes e segurança da informação.		X		
Os colaboradores recebem instruções e orientações sobre os riscos e incidentes de segurança da informação		X		
Os incidentes de segurança são tratados de maneira priorizada.			X	
Maturidade Nível 3				
A política de segurança da informação orienta a organização no escalonamento e reporte de incidentes.			X	
Existe um canal para a comunicação de eventos específicos de segurança da informação				X
As equipes de resposta a incidentes são especificamente treinadas.			X	
Os colaboradores sabem identificar fragilidades de segurança da informação.				X
Maturidade Nível 4				
Existem indicadores de eventos e fragilidades de segurança da informação;			X	
A monitoração sobre recursos críticos de TI são proativos.			X	
Existem treinamentos e programas de conscientização periodicamente.			X	
Maturidade Nível 5				
A análise dos históricos de eventos de segurança faz parte das estratégias de segurança da informação.				X
Existem metas e gerenciamento sobre os eventos e relatos de segurança.			X	
Ferramentas automatizadas para inteligência são de uso frequente.			X	

DESCRIÇÃO DO PROCESSO

GES02 – Gestão de Incidentes de Segurança da Informação e Melhorias

Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação. Convém que responsabilidades e procedimentos estejam definidos para o manuseio efetivo de eventos de segurança da informação.

OBJETIVOS DE CONTROLE

GES02.1 – Responsabilidades e Procedimentos

Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

GES02.2 – Aprendendo com os incidentes de segurança da informação

Convém que sejam estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.

GES02.3 – Coleta de evidências

Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidentes de segurança da informação, envolver uma ação legal (civil ou criminal), convém que evidências sejam coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição(ões) pertinente(s).

MODELO DE MATURIDADE

GES02 – Gestão de Incidentes de Segurança da Informação e Melhorias

0 Não existente quando
A organização não possui ações específicas sobre os incidentes de segurança da informação, assim como não consegue alocar responsabilidades ou definir a necessidade de investigação ou auto aprendizado.

1 Inicial/*Ad Hoc* quando
A segurança da informação é incipiente e apenas algumas responsabilidades podem ser alocadas. Os usuários seguem políticas simples, mas que não estão totalmente formalizadas nos procedimentos de execução. Os incidentes são tratados apenas com a visão corretiva, sem a preocupação em melhoria ou adequação. Não existe a preocupação com a coleta de evidências.

2 Repetível mas intuitivo quando
Existem procedimentos definidos para o tratamento da segurança da informação, mas que são seguidos casualmente e sem controles específicos. Os incidentes são revisados, buscando levar a uma base de conhecimento. A coleta de evidências acontece somente quando existe uma motivação mais forte, ou que possa servir como proteção a organização.

3 Definido quando
Procedimentos foram padronizados e documentados. Responsabilidades são formalmente atribuídas. Os colaboradores assinam os termos de responsabilidade e assumem o conhecimento sobre as políticas, penalizações e procedimentos. Os incidentes possuem tratamento diferenciado e alimentam uma base de conhecimento formal. A coleta de evidências é executada para algumas categorias de incidentes, independente da motivação da organização.

4 Gerenciado e Mensurável quando
Os incidentes de segurança da informação são acompanhados através de indicadores, que também reportam quais os grupos de colaboradores mais ativos no tema. A base de conhecimento acelera a resolução de incidentes e apoia a predição de eventos. O gerenciamento de segurança da informação monitora pontualmente alguns tipos de incidentes, principalmente os de alto risco a continuidade da organização.

5 Otimizado quando
O monitoramento de incidentes é ativo, disparando gatilhos de ações gerenciais. A coleta de evidências é padrão para certas categorias de incidentes e são utilizadas, em conjunto com as responsabilidades, para ações adequadas (judiciais ou não). A gestão de segurança da informação está alinhada com a gestão organizacional.

QUESTIONÁRIO DE MATURIDADE

GES02 – Gestão de Incidentes de Segurança da Informação e Melhorias

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existe alocação de responsabilidade relacionada a segurança da informação.		X		
Os colaboradores seguem políticas simples de segurança da informação.			X	
Os incidentes são tratados apenas com a visão corretiva, sem a preocupação em melhoria ou adequação.		X		
Existe coleta de evidências nos incidentes de segurança da informação.		X		
Maturidade Nível 2				
Existem procedimentos definidos para o tratamento da segurança da informação.		X		
Os incidentes são revisados, buscando levar a uma base de conhecimento.		X		
A coleta de evidências acontece somente quando existe uma motivação mais forte, ou que possa servir como proteção a organização.			X	
Maturidade Nível 3				
Os colaboradores são formalmente treinados e responsabilidades são atribuídas de forma direta (termos de responsabilidade)			X	
Os incidentes possuem tratamento diferenciado e alimentam uma base de conhecimento formal				X
A coleta de evidências é executada para algumas categorias de incidentes.			X	
Maturidade Nível 4				
Existem indicadores de gerenciamento dos incidentes de segurança.			X	
A base de conhecimento acelera a resolução de incidentes e apoia a predição de eventos.			X	
O gerenciamento de segurança da informação monitora alguns tipos de incidentes, principalmente os de alto risco a continuidade da organização.				X
Maturidade Nível 5				
O monitoramento de incidentes é ativo, disparando automaticamente ações gerenciais.				X
A segurança da informação é alinhada com a gestão organizacional.			X	
A coleta de evidências é comum a qualquer tipo de incidente de segurança.			X	

DESCRIÇÃO DO PROCESSO

GES03 – Monitoramento de Atividades

Detectar atividades não autorizadas de processamento da informação. Convém que os sistemas sejam monitorados e eventos de segurança da informação sejam registrados e reportados.

OBJETIVOS DE CONTROLE

GES03.1 – Registros de auditoria
Convém que registros (logs) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.

GES03.2 – Monitoramento do uso do sistema
Convém que sejam estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento sejam analisados criticamente, de forma regular.

GES03.3 – Proteção das informações dos registros (log)
Convém que os recursos e informações de registros (log) sejam protegidos contra falsificação e acesso não autorizado.

GES03.4 – Registros (log) de administrador e operador
Convém que as atividades dos administradores e operadores do sistema sejam registradas.

GES03.5 – Registros (log) de falhas
Convém que as falhas ocorridas sejam registradas e analisadas, e que sejam adotadas ações apropriadas.

GES03.6 – Sincronização dos relógios
Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma fonte de tempo precisa e acordada.

MODELO DE MATURIDADE

GES03 – Monitoramento de Atividades

0 Não existente quando
A organização não organiza ou realiza os registros de atividades de usuários, sistemas. Não há iniciativa de registros, nem mesmo para fins de auditoria.

1 Inicial/*Ad Hoc* quando
Algumas das atividades dos sistemas são sistematicamente registradas, mas não existe análise ou mesmo controle sobre os registros. Os sistemas não estão temporalmente sincronizados. Os registros criados servem apenas para verificação, quando possível de incidentes de pouca gravidade.

2 Repetível mas intuitivo quando
O monitoramento dos sistemas é mais eficiente, mas os registros dependem dos analistas responsáveis e são armazenados de maneira semelhante, mas com fins diferentes. Os processos de auditoria são apenas superficiais e não um controle externo relacionado aos registros. Já existe a preocupação da sincronização dos relógios dos sistemas, mas não é de forma estruturada e confiável.

3 Definido quando
Foram definidos procedimentos para o registro de atividades e principalmente para seu armazenamento. Não existem análises periódicas dos registros, mas quando realizadas conseguem se mostrar efetivas e utilizáveis.

4 Gerenciado e Mensurável quando
A monitoração dos sistemas é parte integrante de atividades rotineiras, os sistemas possuem seus relógios sincronizados e auditorias acontecem em períodos definidos. Indicadores de ocorrências são gerados e reportados a gerência da organização. A análise dos registros é reativa a eventos, mas abrangente e objetiva.

5 Otimizado quando
A monitoração é proativa e os registros são constantemente analisados. Alertas são gerados automaticamente e ações de análises e correções, quando necessários, são ágeis e eficientes. O gerenciamento de incidentes e problemas (ITIL) é suportado pelas atividades de gerenciamento. Indicadores de desempenho dos sistemas são constantemente avaliados, dando suporte a capacidade de processamento da organização. A segurança da informação utiliza o monitoramento como ferramenta de predição e detecção de eventos ativamente.

QUESTIONÁRIO DE MATURIDADE

GES03 – Monitoramento de Atividades

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
As atividades dos sistemas são sistematicamente registradas		X		
Existe análise dos registros das atividades dos sistemas.	X			
Os registros criados servem apenas para verificação de anormalidades		X		
Maturidade Nível 2				
Existe o conceito de monitoração dos sistemas e ambientes.			X	
As análises das monitorações são reativas aos alertas e incidentes		X		
Os processos de auditoria são apenas superficiais na monitoração		X		
Alguns sistemas possuem sincronização de relógios via NTP		X		
Maturidade Nível 3				
A monitoração e registros de atividades possuem procedimentos formais e os colaboradores são devidamente treinados e comunicados.			X	
Existem análises periódicas de registros de sistemas.		X		
Procedimentos de auditoria são executados rotineiramente.			X	
Todos os sistemas possuem sincronização de relógios via NTP		X		
Maturidade Nível 4				
Todos os sistemas possuem sincronização de relógios via NTP				X
Indicadores de monitoração são gerados e reportados a gerência da organização para ações e decisões.			X	
A análise dos registros é reativa a eventos, mas abrangente e objetiva.			X	
Maturidade Nível 5				
A monitoração é proativa e os registros são constantemente analisados.				X
Alertas são gerados automaticamente e ações de análises e correções, quando necessários, são ágeis e eficientes.			X	
O gerenciamento de incidentes e problemas (ITIL) é suportado pelas atividades de monitoração e registro de atividades.				X
Indicadores de desempenho dos sistemas são constantemente avaliados e metas são especificadas.			X	

DESCRIÇÃO DO PROCESSO

GES04 – Aspectos da Gestão da Continuidade de Negócios em Segurança

Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso. Convém que o processo de gestão de continuidade de negócio seja implementado para minimizar um impacto sobre a organização e recuperar perdas de ativos da informação.

OBJETIVOS DE CONTROLE

GES04.1 – Incluindo segurança da informação no processo de gestão da continuidade de negócio
Convém que um processo de gestão seja desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.

GES04.2 – Continuidade de negócios e análise/avaliação de riscos
Convém identificar os eventos que podem causar interrupções aos processos de negócio, junto a probabilidade e impacto de tais interrupções e as consequências para a segurança da informação.

GES04.3 – Desenvolvimento e implementação
Convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos de negócio.

GES04.4 – Estrutura do plano de continuidade de negócios
Convém que uma estrutura básica dos planos de continuidade do negócio seja mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.

GES04.5 – Testes, manutenção e reavaliação dos planos de continuidade de negócio
Convém que os planos de continuidade do negócio sejam testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

MODELO DE MATURIDADE

GES04 – Aspectos da Gestão da Continuidade de Negócios em Segurança

0 Não existente quando
A organização não está sensibilizada com o processo de continuidade de negócios. Não existe uma visão de continuidade, apenas de contingencia (*backup*).

1 Inicial/*Ad Hoc* quando
Já existe uma visão de continuidade de negócios, mas a organização não possui estrutura técnica e organizacional para possuir planos. As iniciativas existentes são pontuais e levam em consideração necessidades individuais.

2 Repetível mas intuitivo quando
As ações de continuidade de negócios atendem requisitos de tecnologia da informação, mas não se estendem a organização como um todo. Os planos desenvolvidos possuem caráter de Plano de continuidade de serviços de TI (PCSTI). Ainda existem poucas iniciativas de testes, sendo mais pontuais do que gerais. A continuidade continua sendo um assunto de TI.

3 Definido quando
A continuidade de negócios foi estendida a toda organização. As pessoas já estão conscientizadas da necessidade da continuidade e o que ela significa. Os planos de continuidade avaliam os riscos de TI e alguns riscos organizacionais e desastres. Treinamentos e testes já são realizados, mas ainda não de forma periódica. A manutenção do plano está focada em manter os ativos de TI em conformidade. Existe uma aderência muito forte ao processo DS4 do COBIT.

4 Gerenciado e Mensurável quando
A continuidade já é um assunto tratado na gerência da organização. A tecnologia da informação é a principal área do plano, mas ele já está alinhado com as expectativas e ações de continuidade de outras áreas, como RH e Financeiro. Existem indicadores de continuidade e constantemente são reportados a gerência atividades previstas nos planos, como testes e o versionamento.

5 Otimizado quando
Os procedimentos e monitoração foram automatizados, gerando alertas de falhas e ativando gatilhos de tomada de decisão. A continuidade é tratada diariamente dentro da organização e seus indicadores estão relacionados a disponibilidade das operações de negócio. A organização sofre auditorias relacionadas a continuidade e as evidências demonstram forte aderência as boas práticas internacionais. A segurança da informação está diretamente relacionada com as iniciativas de continuidade de negócios.

QUESTIONÁRIO DE MATURIDADE

GES04 – Aspectos da Gestão da Continuidade de Negócios em Segurança

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
As iniciativas possuem mais um caráter de contingência do que de continuidade de negócios.		X		
Existem planos de recuperação do ambiente de tecnologia da informação.	X			
A visão de contingência, continuidade e disponibilidade é a mesma.		X		
Maturidade Nível 2				
As ações de continuidade de negócios atendem requisitos de tecnologia da informação		X		
Existem poucas iniciativas de testes, sendo mais pontuais do que gerais.	X			
A continuidade de negócios é vista como responsabilidade da TI.		X		
Maturidade Nível 3				
A continuidade de negócios é comunicada a todos, assim como seus resultados e ações.				X
Existe uma visão forte de gestão de riscos de TI e organizacionais.				X
Treinamentos e testes são realizados de forma total.			X	
Existe uma aderência muito forte ao processo DS4 do COBIT.			X	
Maturidade Nível 4				
A continuidade é um assunto tratado na alta gerência da organização.			X	
A tecnologia da informação é a principal área do plano, alinhado com as expectativas e ações de continuidade de outras áreas, como RH e Financeiro.			X	
Existem indicadores de continuidade e constantemente são reportados				X
Maturidade Nível 5				
Os procedimentos e monitoração da continuidade são automatizados				X
A continuidade é tratada diariamente dentro da organização e seus indicadores estão relacionados a disponibilidade das operações de negócio.			X	
A organização sofre auditorias relacionadas a continuidade de negócio.				X
A segurança da informação está relacionada com a continuidade de negócios.			X	

DESCRIÇÃO DO PROCESSO

GES05 – Conformidade com Requisitos Legais

Evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.

OBJETIVOS DE CONTROLE

GES05.1 – Identificação da legislação aplicável

Convém que todos os requisitos estatutários, regulamentares e contratuais pertinentes, e o enfoque as organização para atender a esses requisitos, sejam explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação da organização.

GES05.2 – Direitos de propriedade intelectual

Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de software proprietários.

GES05.3 – Proteção de registros organizacionais

Convém que registros importantes sejam protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

GES05.4 – Proteção de dados e privacidade de informações pessoais

Convém que a privacidade e a proteção de dados sejam asseguradas conforme exigido nas legislações, regulamentações e, se aplicável, nas cláusulas contratuais pertinentes.

GES05.5 – Prevenção de mau uso de recursos de processamento da informação

Convém que os usuários sejam dissuadidos de usar recursos de processamento da informação para propósitos não autorizados.

GES05.6 – Regulamentação de controles de criptografia

Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos e regulamentações pertinentes.

MODELO DE MATURIDADE

GES05 – Conformidade com Requisitos Legais

0 Não existente quando
Não existe a preocupação, por parte da organização, relacionada a conformidade com requisitos legais como normas, estatutos, leis, regulamentações ou contratos, no que diz respeito a segurança da informação.

1 Inicial/*Ad Hoc* quando
A organização desenvolveu controles de conformidade que abrange principalmente contratos com terceiros e clientes. Algumas iniciativas de proteção de informações pessoais já são aplicadas de ainda de maneira pontual.

2 Repetível mas intuitivo quando
Os processos e controles relacionados a contratos e legislação em vigor evoluíram ao ponto de toda a organização consultar o departo jurídico sobre o assunto. As informações pessoais ainda não são devidamente protegidas e vazamentos de informações podem ocorrer. Os recursos de processamento de informação são monitorados e seu uso é controlado pelas equipes de tecnologia da informação. A organização faz campanhas contra pirataria de software e direitos intelectuais.

3 Definido quando
A organização definiu e publicou políticas relacionadas a conformidade com leis, regulamentações e contratos. Os colaboradores foram devidamente informados dos procedimentos a serem executados. O uso de recursos computacionais é fortemente monitorado e as informações sensíveis de clientes e fornecedores é protegida e de acesso restrito.

4 Gerenciado e Mensurável quando
Controles e monitorações são realizados sobre as informações pessoais. Indicadores mostram a aderência da organização no atendimento a normas e a conformidade com auditorias relacionadas a normas, regulamentações e leis. A gerência monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando muito bem. Alguns processos de controle já demanda a necessidade de automação.

5 Otimizado quando
Existe um forte controle nos sistemas de informação em relação ao acesso a informações sensíveis, como dados pessoais. Além disso, a monitoração é proativa no que diz respeito a etapas de processos e atendimento a normas e regulamentações. O gerenciamento de conformidade é realizado por uma equipe dedicada e apoiada por empresas externas de consultoria. Auditorias independentes são executadas periodicamente a fim de avaliar os controles e sua eficiência.

QUESTIONÁRIO DE MATURIDADE

GES05 – Conformidade com Requisitos Legais

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Iniciativas de proteção de informações pessoais já são aplicadas, mas ainda de maneira pontual.	X			
Existem controles de conformidade que abrange principalmente contratos com terceiros e clientes		X		
Maturidade Nível 2				
Existe consulta ao departamento jurídico em relação a contratos e legislação em vigor.			X	
Informações sensíveis são protegidas com vazamentos e perdas.		X		
Os recursos de processamento de informação são monitorados e seu uso é controlado pelas equipes de tecnologia da informação.		X		
A organização faz campanhas contra pirataria de software e direitos intelectuais.			X	
Maturidade Nível 3				
A organização definiu, publicou e conscientizou sobre políticas relacionadas a conformidade com leis, regulamentações e contratos				X
O uso de recursos computacionais é fortemente monitorado.			X	
Informações sensíveis de clientes e fornecedores são protegidas e restritas			X	
Maturidade Nível 4				
Indicadores mostram a aderência da organização no atendimento as normas e legislação em vigor.			X	
Existem controles automatizados na gestão de riscos (GRC).			X	
Controles e monitorações são realizados sobre as informações sensíveis.				X
Maturidade Nível 5				
Existe monitoração proativa no que diz respeito a etapas de processos e atendimento a normas e regulamentações				X
O gerenciamento de conformidade é realizado por uma equipe dedicada e apoiada por empresas externas de consultoria.			X	
Auditorias independentes são executadas periodicamente a fim de avaliar os controles e sua eficiência.				X

DESCRIÇÃO DO PROCESSO

GES06 – Conformidade com Normas, Políticas de Segurança da Informação e Conformidade Técnica

Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação. Convém que a segurança dos sistemas de informação seja analisada criticamente a intervalos regulares.

OBJETIVOS DE CONTROLE

GES06.1 – Conformidade com as políticas e normas de segurança da informação

Convém que gestores garantam que todos os procedimentos de segurança da informação dentro da sua área de responsabilidade estão sendo executados corretamente para atender à conformidade com as normas e políticas de segurança da informação.

GES06.2 – Verificação da conformidade técnica

Convém que sistemas de informação sejam periodicamente verificados em sua conformidade com as normas de segurança da informação implementadas..

MODELO DE MATURIDADE

GES06 – Conformidade com Normas, Políticas de Segurança da Informação e Conformidade Técnica

0 Não existente quando
A organização não possui definidas normas e/ou políticas de segurança da informação que exijam dos sistemas conformidade.

1 Inicial/*Ad Hoc* quando
Alguns sistemas de informação possuem procedimentos básicos de segurança da informação e estes procedimentos seguem especificações de normas e regulamentos internos. Mesmo assim, os procedimentos não são verificados e/ou auditados. Os responsáveis pelos sistemas não reportam ou medem a aderência as normas internas aos seus gestores.

2 Repetível mas intuitivo quando
Os gestores da organização já se preocupam que os sistemas sigam as normas e políticas de segurança da informação, mas ainda de maneira pontual e com critérios individuais. Os procedimentos de auditoria interna apenas verificam se existem políticas e normas e não necessariamente a efetividade de sua aplicação.

3 Definido quando
A organização possui procedimentos padronizados para a aplicação de normas e políticas de segurança. Nestes procedimentos estão inclusas as questões de auditoria, mas mesmo assim a periodicidade definida não é seguida e depende da necessidade de cada sistema. Os gerentes de sistemas são formalmente responsabilizados pelas questões de segurança da informação.

4 Gerenciado e Mensurável quando
Os sistemas de informação possuem auditorias periódicas que são aprovadas e homologadas pelos gestores responsáveis. A aderência a normas e políticas internas é avaliada nas auditorias e desvios são formalmente reportados a alta direção da organização. Existe um calendário geral de auditoria e requisitos a serem atendidos.

5 Otimizado quando
O processo de auditoria nos sistemas é baseado em ferramentas automatizadas que reportam não conformidades e geram incidentes de segurança da informação automaticamente. Os gerentes possuem indicadores do grau de aderência dos sistemas as normas e políticas internas que são reavaliados a cada mudança autorizada. O calendário de auditoria é seguido e reportado a alta gerência da organização.

QUESTIONÁRIO DE MATURIDADE

GES06 – Conformidade com Normas, Políticas de Segurança da Informação e Conformidade Técnica

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Os sistemas possuem procedimentos básicos de segurança da informação.		X		
Os procedimentos seguem normas e regulamentos internos.	X			
Existem responsáveis alocados aos sistemas de informação.		X		
Maturidade Nível 2				
Os procedimentos de auditoria interna verificam se existem políticas e normas para os sistemas.			X	
Os procedimentos dos sistemas seguem normas e regulamentos internos				X
Maturidade Nível 3				
Existem procedimentos padronizados para a aplicação de normas e políticas de segurança				X
Os gerentes de sistemas são formalmente responsabilizados pelas questões de segurança da informação			X	
Procedimentos de auditorias são periódicos nos sistemas de informação.				X
Maturidade Nível 4				
Os sistemas de informação possuem auditorias periódicas que são aprovadas e homologadas pelos gestores responsáveis.				X
A aderência a normas e políticas internas é avaliada nas auditorias e desvios são formalmente reportados a alta direção da organização.			X	
Existe um calendário geral de auditoria e requisitos a serem atendidos.			X	
Maturidade Nível 5				
A auditoria nos sistemas é baseada em ferramentas automatizadas.				X
Não conformidades geram incidentes de segurança da informação automaticamente.			X	
Os gerentes possuem indicadores do grau de aderência dos sistemas as normas e políticas.			X	

DESCRIÇÃO DO PROCESSO

GES07 – Considerações quanto a Auditoria de Sistemas de Informação

Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação. Convém que existam controles para a proteção dos sistemas operacionais e ferramentas de auditoria durante as auditorias de sistema de informação.

OBJETIVOS DE CONTROLE

GES07.1 – Controles de auditoria de sistemas de informação

Convém que requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos de negócio.

GES07.2 – Proteção de ferramentas de auditoria de sistemas de informação

Convém que o acesso às ferramentas de auditoria de sistema de informação seja protegido, para prevenir qualquer possibilidade de uso impróprio ou comprometimento.

MODELO DE MATURIDADE

GES07 – Considerações quanto a Auditoria de Sistemas de Informação

0 Não existente quando
Não existe um processo de auditoria ou controles de auditoria implementados nos sistemas de informação.

1 Inicial/*Ad Hoc* quando
A organização possui alguns controles de auditoria nos sistemas de informação, mas baseados apenas no controle de acesso as aplicação e não em trilhas de auditorias. As ferramentas de auditoria são básicas e dependem muito da habilidade dos gestores de sistemas para seu uso correto.

2 Repetível mas intuitivo quando
Os sistemas de informação passam por processos de auditorias, mas a coleta de evidências é baseada em solicitações pontuais e na maioria das vezes se restringe a controle e perfil de acesso aos sistemas. Existem ferramentas de auditorias que são aplicadas em alguns sistemas e seu uso e acesso é de responsabilidade da equipe de segurança da informação da organização.

3 Definido quando
Os sistemas de informação geram informações de auditoria de maneira padronizada, seguindo os requisitos de auditoria estabelecidos. A cada novo requisito é realizada uma análise de impacto para não oferecer risco de interrupção dos sistemas de negócio. As ferramentas de auditoria geram informações completas, mas que não são analisadas constantemente pelas equipes de segurança. Existem iniciativas de indicadores pontuais relacionados as poucas análises realizadas.

4 Gerenciado e Mensurável quando
A gerência monitora e mede a aderência aos procedimentos de auditoria aos trilhões de auditoria colocados nos sistemas. As informações de auditoria são analisadas constantemente e existem indicadores formais de aderência aos requisitos de auditoria. As ferramentas de auditoria são de uso restrito as equipes de segurança da informação e equipes de auditoria interna.

5 Otimizado quando
Alertas automatizados são gerados quando as ferramentas de auditoria detectam não conformidades nos sistemas de informação. Estes alertas são comunicados as gerências de sistemas e de segurança da informação. Os indicadores são refinados a um nível de boas práticas. As ferramentas de auditoria possuem acesso restrito que também é auditado.

QUESTIONÁRIO DE MATURIDADE

GES07 – Considerações quanto a Auditoria de Sistemas de Informação

	Somente em algumas situações	Em toda Tecnologia da Informação na Organização	Em vários departamentos da organização, inclusive TI	Em toda Organização
Maturidade Nível 1				
Existem controles de auditoria nos sistemas de informação.		X		
Os controles de auditoria são baseados no acesso as aplicações.		X		
As ferramentas de auditoria são básicas e dependem muito da habilidade dos gestores de sistemas para seu uso correto.	X			
Maturidade Nível 2				
A coleta de evidências é baseada em solicitações pontuais e na maioria das vezes se restringe a controle e perfil de acesso aos sistemas.			X	
Existem ferramentas de auditorias que são aplicadas nos sistemas		X		
O uso das ferramentas são de responsabilidade da segurança da informação.			X	
Maturidade Nível 3				
Os sistemas de informação geram informações de auditoria de maneira padronizada, seguindo os requisitos de auditoria estabelecidos.				X
Para cada novo requisito é realizada uma análise de impacto para não oferecer risco de interrupção dos sistemas de negócio			X	
O processo de auditoria é formalmente informado e treinado.			X	
Maturidade Nível 4				
A gerência monitora e mede a aderência aos procedimentos de auditoria as trilhas de auditoria colocadas nos sistemas				X
As informações de auditoria são analisadas constantemente e existem indicadores formais de aderência aos requisitos de auditoria.				X
As ferramentas de auditoria são de uso restrito as equipes de segurança da informação e equipes de auditoria interna.			X	
Maturidade Nível 5				
Alertas automatizados são gerados quando as ferramentas de auditoria detectam não conformidades.				X
As ferramentas de auditoria possuem acesso restrito que também é auditado.			X	
Não conformidades são comunicadas as gerências de sistemas e de segurança da informação				X