UNIVERSIDADE FEDERAL DE MINAS GERAIS
FACULDADE DE CIÊNCIAS ECONÔMICAS

Rodrigo Gabrich Cota

AUDITORIA DE SISTEMAS APLICATIVOS DE NEGÓCIOS

Belo Horizonte
2015

RODRIGO GABRICH COTA

AUDITORIA DE SISTEMAS APLICATIVOS DE NEGÓCIO

Monografia apresentada no Centro de Pós—graduação e pesquisa em contabilidade de Controladoria – CEPCON - no curso Especialização em Auditoria Externa da Faculdade de Ciências Econômicas, da Universidade Federal de Minas Gerais, como requisito parcial para a obtenção do certificado de Especialista em Auditoria Externa.

Orientador: Afonso Felício Kalil Filho

BELO HORIZONTE

2015

Universidade Federal de Minas Gerais
Faculdade de Ciências Econômicas
Programa de Pós-Graduação

Trabalho de Conclusão de Curso de Especialização em auditoria externa intitulada *Auditoria em Sistemas Aplicativos de Negócios*, de autoria de Rodrigo Gabrich Cota, aprovada pela banca examinadora constituída pelos seguintes professores:

_____

Prof. Dr. ***
instituição

_____

Prof. Dr. ***
instituição

_____

Prof. Dr. ***
instituição

_____

Prof. Dr. ***
instituição

_____

Prof.ª Laura Edith Taboada Pinheiro
Coordenador (a) do Núcleo de Informação Tecnológica e Gerencial – NITEG
ECI/UFMG

Data de aprovação: Belo Horizonte, de ..... de 20.....

AGRADECIMENTOS

À DEUS, por tudo que pude realizar na vida, incluindo essa nova formação.

À Universidade Federal de Minas Gerais, ao meu orientador, Professor Afonso Felício Kalil Filho, pelas críticas e apoio em ideias e uma das principais fontes de informação que tive no curso.

Aos colegas de curso, importantíssimos no processo de aprendizagem durante essa caminhada.

Aos meus pais Maria Socorro Gabrich Cota e Carlos Cota Rodrigues, pelo seu inigualável apoio.

E a todos aqueles que contribuíram de alguma maneira para a minha formação.

RESUMO

É certo que não se ouvia falar em auditoria de Sistemas de Informação antes da existência dos sistemas informatizados. Esse modelo de auditoria encontrou seu espaço com a adoção dos computadores pelas empresas e na evolução dos meios de comunicação. O presente trabalho propõe uma metodologia de auditoria baseada no modelo referencial metodológico ISO/IEC 27002, bem como em padrões e normas de melhores práticas aplicáveis às empresas do ramo da construção civil, mas que pode ser adaptado à qualquer setor empresarial. Através da metodologia será possível avaliar os Sistemas de Informação relacionados ao negócio quanto à sua integridade, segurança, eficiência e eficácia. Paralelamente foi realizado um estudo de conceitos, modelos, padrões e normas de auditoria aplicáveis aos Sistemas de Informação. Como estudo de caso, um questionário foi elaborado a fim de identificar o quanto as empresas do ramo da construção civil estão preocupadas com seus Sistemas Aplicativos de Negócios. Ressaltamos também as referências metodológicas - consideradas as mais modernas que fundamentam as “boas práticas” no mercado e as mais utilizadas atualmente em todo o mundo pelas organizações - que fundamentaram, no seu conjunto, a confecção deste trabalho.

Palavras chave: COBIT, ITIL, COSO, CMMI.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas.

BCI – "*Business Continuity Institute*" – (Instituto de Continuidade Negócios) – entidade internacional que define as boas práticas em relação à continuidade de negócios. Inclui informações sobre planos de desastre ("*disaster recovery*") e planos de contingência.

CMM – "*Capability Maturity Model*" do "*Software Engineering Institute*". (Modelo de Capacidade de Maturidade do Instituto de Engenharia de Software").

CMMI – "*Capability Maturity Models Integration*" (Integração de Modelos de Capacidade de Maturidade).

CobiT – "*Control Objectives for Information and related Technology*", (Objetivos de Controle para a Informação e Tecnologia a ela relacionada), de propriedade do Instituto de Governança de TI – ("ITGI" – *"Information Tecnhology Governance Institute"*) fornece boas práticas que representam o consenso de especialistas, focado mais nos controles do que na execução e está baseada em um modelo de domínios e processos, apresentando as atividades em uma estrutura lógica e gerenciável.

COSO – "*Committee of Sponsoring Organizations*" of Treadway Commission's - (Comitê das Organizações Promotoras da Comissão *Treadway*) Internal Control Integrated Framework – (Modelo Integrado de Controles Internos).

DRP – *"Disaster Recovery Plan"* (Plano de Recuperação de Desastres).

ERM – *"Enterprise Risk Management"* (Gestão de Riscos Empresariais).

ERP – *"Enterprise Resource Planning"* (Planejamento de Recursos Corporativos) – conjunto de programas desenvolvidos para integrar todos os dados e processos de uma organização.

IEC – *"International Eletrotechnical Comission"* (Comissão Internacional de Eletrotécnica).

ISACA – *"Information System Audit and Control Association"* Associação internacional, independente e sem fins lucrativos, sediada em Illinois, EUA. Está representada em cerca de 180 países, com 140.000 profissionais associados (vide www.isaca.org).

ISMS – *"Information Security Management System"* (Sistema Gerencial da Segurança da Informação).

ISO – *"International Standardization Organization"* (Organização de Padronização Internacional).

ISO/IEC 27000 – Família de Normas relacionadas à Segurança da Informação.

ISO/IEC 27001 – Padrão de especificação para um Sistema Gerencial da Segurança da Informação.

ISO/IEC 27002 – Padrão de procedimentos e sugestões de Segurança da Informação. Corresponde à ABNT 17799.

ISO/IEC 27003 – Guia de implantação do Sistema Gerencial da Segurança da Informação.

ISO/IEC 27004 – Padrão de medição e métricas para o Sistema Gerencial da Segurança da Informação.

ISO/IEC 27005 – Padrão para Gestão de Risco em Segurança da Informação.

ISO/IEC 27006 – Guias para organizações certificadoras de Certificação em Gestão da Segurança da Informação.

ITGI – *"IT Governance Institute"* (Instituto de Governança de TI), estabelecido em 1998 pela ISACA (vide Sigla) para melhoria do pensamento e dos padrões internacionais de direção e controle da tecnologia da informação nas organizações.

ITIL - *"Information Technology Infrasctructure Library"* (Biblioteca de Infraestrutura da Tecnologia da Informação).

PAC – Plano de Administração de Crises.

PCN – Plano de Continuidade de Negócios.

PCO – Plano de Continuidade Operacional

PRD – Plano de Recuperação de Desastre.

PMBOK – *"Project Management Body of Knowledge"* (Conjunto de Conhecimentos de Gerenciamento de Projetos).

SAN – Sistemas Aplicativos de Negócios – atendem às áreas de negócios de uma organização.

SAP – Sistemas, Aplicações e Produtos em Processamento de Dados – em tradução livre. A desenvolvedora do software é alemã, sendo assim o nome original é *"Systeme, Anwendugen und Produkte in der Datenverarbeitung".* Em inglês é *"Systems Applications and Products in Data Processing"*.

SGSI – Sistema Gerencial da Segurança da Informação.

SLA – *"Service Level Agreement"* (Acordo de Nível de Serviço).

SLM – *"Service Level Management"* (Gestão do Nível de Serviço).

TI – Tecnologia da Informação.

TIC – Tecnologia da Informação e Comunicação – termo cada vez mais utilizado na área de informática por englobar o universo das comunicações, essenciais no mundo moderno.

1. Sumário

1. Introdução

A tecnologia da informação e comunicação – "TIC" - vem apresentando um enorme progresso nos últimos tempos. Isto se reflete na maneira como as informações são circuladas, principalmente pelas mídias magnéticas, nos processos contábeis e financeiros, nas operações de fabricação, marketing, venda, recursos humanos, etc., e no gerenciamento de todos os seus processos.

Obviamente que há uma necessidade imperiosa de monitorar, avaliar e tomar decisões importantes por parte de seus Gestores. Daí surge a real demanda por uma governança, baseada nos controles internos de todos os processos, com o objetivo de identificar as vulnerabilidades existentes, minimizar os riscos ao negócio, aperfeiçoar a produtividade das instituições, aumentar a agilidade e eficácia na prestação de serviços, e melhorar a maneira como os agentes externos, principalmente os clientes, enxergam uma organização.

De forma geral, as novas ferramentas de gestão, desenvolvidas nos últimos dez anos, em conjunto com as tecnologias, cada vez mais sofisticadas e rápidas, têm produzido um impacto bastante significativo nas instituições e seus clientes.

Toda organização, independentemente do seu tamanho, do segmento onde atua (comércio, indústria, financeiro, etc.), seja pública ou privada, tende a aumentar sua dependência pela tecnologia da informação e comunicações. Praticamente todas elas dependem de sistemas automatizados para administrar suas operações e fornecer subsídios para planejamento e relacionamento com fornecedores e clientes. Essa crescente dependência de sistemas de informação cria a necessidade de garantir a consistência dos dados inseridos, processados, armazenados e exibidos por sistemas computacionais.

Existem várias partes interessadas nos dados gerados pelos sistemas automatizados, sendo eles agentes internos ou externos da organização. Há também as partes impactadas por algum processo automatizado que junto com os interessados, constituem o que se denomina como "*stakeholders*" (clientes, acionistas, usuários, fornecedores, etc.). Para garantir a consistência desses dados diversos tipos de auditoria podem ser usados, dentre eles a auditoria de sistemas e, especificamente, a auditoria de Sistemas Aplicativos de Negócios.

Assim como uma auditoria financeira verifica balanços monetários e práticas contábeis, uma auditoria de sistemas analisa a integridade de sistemas eletrônicos. Esse tipo de auditoria é bastante abrangente, considerando a dependência das empresas em sistemas computacionais.

Entretanto, existem diversos mecanismos de controle extremamente simples que não demandam profundo conhecimento na área de “TIC” e que podem auxiliar os gestores responsáveis pelos sistemas aplicativos das empresas.

1.1 Problema

Qual a percepção que os responsáveis pela gestão da tecnologia da informação das empresas têm em relação aos ativos computacionais?

Um dos grandes desafios para garantir a eficácia da gestão tem sido a aplicação de auditorias dos processos. Assim sendo, é necessário garantir que essas auditorias sejam eficazes e para tanto é necessário analisar os melhores métodos para as mesmas. No caso específico de auditorias em softwares e aplicativos será admitido por este trabalho o método COBIT, por se tratar de um modelo de governança de que ajuda a entregar valor, compreender e gerenciar os riscos associados a “TIC”.

A maioria das organizações conhece os mais variados tipos de controles que são fundamentais para suas operações, mas não os registram ou, caso os façam, não é de forma estruturada e/ou não os monitoram adequadamente. Assim, por exemplo, se uma empresa tem condições de verificar quais são os indivíduos que tem acesso às informações corporativas necessárias ao negócio, na maioria das vezes não tem uma Política adequada sobre o assunto. Se existe a Política, ou não é atualizada regularmente e/ou não é adequadamente disponível, ou ainda não prevê um processo que garanta a imediata atualização nos casos em que o acesso não é mais necessário.

Para identificar, mesmo que por meio de amostragem, o quanto as companhias estão preocupadas com seus ativos computacionais, foi elaborado um questionário sobre alguns tópicos básicos na área de segurança da informação e controles internos, sendo esse aplicado às empresas ligadas à construção civil.

A análise das respostas e respectivas avaliações podem evidenciar necessidade de maior atenção aos níveis de controle das “TIC”s tanto nesse seguimento de mercado, como em outros. Supõe-se que a área financeira das empresas é aquela que recebe maior atenção e onde os controles são mais contundentes devido à preocupação dos gestores desta área para com o *“core-business”* da organização e o produto ali trabalhado que é, em resumo, a melhor aplicação do produto “DINHEIRO”.

1.2 Objetivos

Este trabalho tem o objetivo de desmistificar a complexidade dos mecanismos básicos de controle, e propõe diversos processos e procedimentos simples, abrangentes, de

fácil implantação e de custos mínimos. Obviamente que o grande postulado da Segurança – “Não há segurança 100% garantida” - continua válido. O que não podemos é deixar de perseguir sempre a meta dos 100%, ainda que esta seja um sonho.

Cremos que, qualquer gestor das áreas de negócio, com responsabilidades de proprietário de um sistema aplicativo (ex: “Contas a Receber”, “Faturamento”, “Compras”, “RH”, “Contabilidade”, “Inventário”, “Cálculos de Engenharia”, Impostos, etc.), ao ler esta proposição, terá melhores condições de gerir a sua área de atuação, aperfeiçoando seus controles e exercendo o monitoramento necessário para identificar as vulnerabilidades nos processos sob sua responsabilidade, entender os problemas, buscar soluções eficazes, rápidas e baratas e tratar adequadamente os riscos que envolvem os seus negócios.

É importantíssimo entender algumas definições e premissas para o bom entendimento deste trabalho, constantes do tópico seguinte a fim de que os jargões sejam completamente assimilados pelo leitor.

O objetivo deste trabalho é, a partir de uma análise preliminar, sinalizar para as empresas as carências de fragilidades a que possam estar expostas e, assim, sugerir método que possa garantir maior consistência e seguridade dos dados de softwares e aplicativos.

1.2.1 Objetivo geral

Identificar e demonstrar a percepção dos gestores quanto à importância dos ativos computacionais e o que é feito para garantir a sua segurança e consistência. Trabalho que sirva para médias e grandes empresas que atuam no mercado da construção civil, com foco estritamente gerencial, sem aprofundamento em assuntos técnicos que demandam muita experiência na área de tecnologia da informação.

1.2.2 Objetivos Específicos

- Revisão dos principais conceitos aplicáveis ao tema.
- Apresentar o panorama atual de controles básicos de segurança da informação e controle de atividades chave nos sistemas aplicativos na maioria das empresas brasileiras, no segmento “Fornecedores de processos de Construção Civil”, identificando as vulnerabilidades e riscos.
- Aperfeiçoamento da Auditoria de Sistemas em Sistemas Aplicativos de modo a possibilitar a sua realização (ainda que na modalidade de revisão técnica) por profissionais que não sejam especialistas em Sistemas de Informação.

• Constituir uma lista de verificação primária - *"checklist"* - que facilite a compreensão e utilização nas empresas para que, de modo rápido, obtenha-se um diagnóstico da situação e as principais medidas a serem tomadas.

Neste último caso, salientamos que o *"checklist"* apresentado neste trabalho é um guia inicial para qualquer tipo e porte de empresa. Ele poderá ser continuamente aperfeiçoado e incrementado, conforme a profundidade dos temas a serem analisados em análises mais detalhadas e à medida que a organização evolua na conscientização e comprometimento com a Segurança da Informação em todos os níveis gerenciais, principalmente no nível da Diretoria. Assim, por exemplo, se existe uma Política de Segurança da Informação formalizada e aprovada, mas não totalmente acessível a todos os usuários e gestores envolvidos, é necessário que se cumpram outros requisitos tais como: disponibilização da Política e a garantia de que todas as pessoas conheçam as normas e procedimentos ali documentados e implantação de controles que assegure que, periodicamente, todos formalizam o entendimento da Política, tenha sido esta atualizada ou não. Estes cuidados evitam que, em casos de desvios às normas de segurança, uma pessoa alegue o desconhecimento das regras e/ou que o seu aceite se deu há muito tempo.

1.3 Justificativa

A pesquisa se justifica pelos fatos já expostos nessa introdução, tanto pela necessidade de uma governança mais aperfeiçoada quanto por fornecer meios para analisar processos informatizados, trazendo maior segurança para as empresas. Consideramos de suma importância a realização de controles internos nos processos, auxiliando a identificação de vulnerabilidades existentes. A partir disso, providenciar as correções para minimizar os riscos ao negócio, melhorar a produtividade das instituições, aumentar a agilidade e eficácia na prestação de serviços e melhorar a maneira como os agentes externos, principalmente os clientes, enxergam uma organização.

1.4 Estrutura da dissertação

Este trabalho é composto por:

a) Esta introdução;
b) Revisão teórica dos principais conceitos e as premissas básicas relacionadas ao tema;
c) As respostas obtidas por meio do questionário aplicado aos gestores de departamentos de tecnologia da informação com alguns comentários deste autor;

d) Tabela – "*Checklists*" – para uma revisão e/ou auditoria da situação de controle da organização no quesito de segurança de sistemas aplicativos de negócios.
e) As considerações finais.

2. Conceitos Gerais e Premissas Básicas

2.1 Sistemas Aplicativos de Negócios – "SAN"

São "softwares" desenvolvidos para executar funções específicas de uma área de negócio da empresa, partindo de definições e parâmetros que norteiam os processos empresariais de negócio. A construção destes softwares deve, também, obedecer aos requerimentos exigidos pelas normas regulatórias e Leis (municipais, estaduais e federais) inerentes à área do mercado em que atua. Assim, por exemplo, um "SAN" que controla os impostos e taxas relativos às negociações de uma organização, deve estar constantemente alinhado com todas as atualizações efetivadas nas esferas governamentais sobre este tema.

Os "SAN" podem ser desenvolvidos internamente ou adquiridos no mercado (através de *"Software Houses"* – ou empresas que desenvolvem sistemas aplicativos). Alguns podem utilizar funções mais sofisticadas, interdepartamentais, abrangendo mais de uma área de negócio, como por exemplo, atendem ao Faturamento, às Contas a Pagar e Contabilidade, onde as informações transitam automaticamente pelas três áreas de negócio. O objetivo é alcançar o melhor sincronismo e rapidez entre as operações, menos redundâncias e repetições e maior confiabilidade nos resultados sistêmicos, permitindo aos gestores uma melhor tomada de decisões.

Um exemplo de "SAN" deste tipo são os "ERP"- *"Enterprise Resource Planning"*, que são conjuntos de procedimentos ou programas padrões, desenvolvidos para integrar todos os dados e processos de uma organização em um único sistema e esta integração pode ser analisada sob a perspectiva funcional (sistema de finanças, contabilidade, recursos humanos, fabricação, marketing, vendas, compras, etc.) e perspectiva sistêmica (sistemas de processamento de transações, de informações gerenciais, de apoio à decisão, etc.).

O "ERP" atua como um centro de controle de toda a organização, coletando as informações sobre a situação e relatórios de andamento de diferentes divisões, e os disponibilizando para outros departamentos. As informações são atualizadas pelos usuários em tempo real e ficam acessíveis a qualquer momento para qualquer pessoa que precisar delas. As decisões se tornam mais seguras, em tempo real e aumentam a produtividade dos usuários.

Nem todas as organizações precisam de todas as funcionalidades disponíveis em um "ERP" e, por isto, as funções são oferecidas em formato modular, o que permite às empresas implantar somente os módulos de que precisam e adicionar outro posteriormente, caso necessário.

Dentre os "ERP" mais conhecidos citamos:

- **SAP ERP:** sistema integrado de gestão empresarial transacional, produto da empresa alemã SAP (“Sistemas, Aplicações e Produtos em Processamento de Dados” – mais detalhes no item Abreviaturas no início deste trabalho) com cerca de 90 mil clientes no mundo, a maioria empresas de grande porte.
- **TOTVS:** líder no Brasil e na América Latina, e considerada a 6ª no mundo. É a controladora das empresas Microsiga, Datasul e RM Sistemas. Produz diversos tipos de “ERP”: “Totvs Protheus”, “Totvs RM”, “Totvs Datasul”, “Totvs Logix” e “Totvs Microempresa”.
- **ORACLE:** além de diversos módulos relativos às áreas de negócios, possui ferramenta para facilitar o uso de aplicações multitarefas pela computação na nuvem, permitindo o lançamento de projetos mais baratos, mais rápidos e de baixo risco. Um dos seus produtos é o “JD Edwards Enterprise One”.

Independentemente da origem do desenvolvimento do “SAN”, da sua abrangência e da área para a qual é desenvolvido, é fundamental que o responsável pelos resultados das funções do processo atendido pelo “SAN”, denominado “Proprietário” (vide a seguir), tenha a documentação completa, mais atualizada possível e aprovada nos níveis competentes. É comum haver atualizações ao longo do ciclo de vida de um “SAN” e, por isto, é primordial que a documentação reflita tempestivamente as alterações feitas. Para efeito deste trabalho, destacamos alguns manuais básicos para o gestor:

- **Manual de Funções do “SAN”:** identificam, resumidamente, as funções e os controles do sistema, permitindo ao Proprietário, uma visão geral das entradas e saídas do sistema sob sua propriedade, os elementos de controle necessários para que a gestão possa ser exercida na linguagem de negócios do proprietário.
- **Manual de Entradas e Saídas do “SAN”:** permite que o proprietário e demais usuários conheçam as informações necessárias para a execução das funções, (“de onde” elas se originam e “como”) bem como os relatórios e demais saídas fornecidas pelo “SAN” (“para onde seguem”). Na parte dos Relatórios, deve ser explicado para cada um, o formato, o tipo de conteúdo e os fechamentos e/ou mecanismos de controle para possibilitar ao usuário uma análise e avaliação dos resultados do processo.

- **Manual de Operações de Negócios do "SAN":** permite que o proprietário conheça todos os mecanismos de controle do aplicativo sob sua propriedade e exerça um eficiente e eficaz monitoramento das atividades chave de gestão do "SAN". Dentre estes controles, destacamos os relacionados aos de qualidade (consistências, fechamentos, totalizações) segurança lógica (administração de usuários, privilegiados ou não, regras de acesso às informações, perfis de segurança) e administrativas (inter-relacionamento com demais processos de negócios e contabilização dos resultados).
- **Manual de Sistemas do Aplicativo "SAN":** detalham os inter-relacionamentos entre o "SAN" e os demais sistemas que lhe fornecem informações (entradas), os que interagem com ele e os que precisam de seus resultados (saídas) para continuar as operações de negócios. Informa também os controles de cada etapa do processo, permitindo visualizar qualquer término inesperado. Indica os pontos em que são necessários *"backups"* para permitir retrabalhos quando for o caso. Os controles servem para garantir a completude adequada do processo bem como para indicar que a saída de uma etapa corresponde à entrada da etapa seguinte (normalmente os controles são focados em totais de conciliação que garantem que nenhuma informação foi "perdida" ou "desconsiderada" na transmissão de uma etapa para outra).

Em alguns ambientes, os manuais acima podem estar condensados em um só Manual. Neste caso, espera-se que contenha minimamente as informações anteriormente descritas, para cada tipo de Manual.

2.2 Proprietário de Sistemas Aplicativos de Negócios

É denominado como "*Owner*" do processo atendido pelo "SAN". Deve ter experiência na área em que atua e conhecer as funções e controles do "SAN", bem como das origens e dos destinos das informações que transitam pelo processo. Deve levar em consideração que os dados de negócio sob sua propriedade só devem ser acessados por quem realmente precisa, atendendo ao princípio fundamental de segurança de acesso que é a necessidade de negócios (em inglês: "*business need*"). O proprietário deve ser o primeiro (e mais importante) "auditor" de seu próprio "SAN", visto que ele como gestor, deve ser o revisor mais preocupado com os controles de seu processo e não o auditor externo (ou interno).

O auditor, normalmente, avalia o processo em bases esparsas, havendo grandes períodos sem uma revisão formal. Por isto, a revisão pelo próprio gestor deve ser exercida diariamente para evitar que um problema assuma proporções indesejáveis.

Caso um processo envolva vários “SAN”s, a propriedade de cada um deles deve ser discutida adequadamente, aprovada e formalizada. Não deve haver “SAN” sem propriedade. Por outro lado, um Proprietário (“Owner”) pode se responsabilizar por mais de um “SAN”.

2.3 Administrador de Segurança de um “SAN”

Indivíduo nomeado formalmente pelo Proprietário do “SAN” para executar funções administrativas de controle de acessos.

Cabe a ele incluir, remover e alterar usuários e seus respectivos poderes de acesso (só leitura, atualização, atualização incluindo eliminação, etc.) exatamente conforme as aprovações formalizadas que lhe são direcionadas pelo Proprietário do “SAN”.

O administrador não é o responsável pela aprovação de um pedido de solicitação, embora possa assessorar o Proprietário na avaliação do pedido.

O indivíduo que tem este poder de “Administrador” torna-se um usuário privilegiado, afinal ele poderá, teoricamente, alterar qualquer permissão de acesso independente do usuário e da ocasião, inclusive o seu próprio. Por isto suas atividades devem ser totalmente registradas, monitoradas e avaliadas. Um procedimento auxiliar, exequível e fácil de implantação para o registro e monitoramento é a gravação de trilha de auditoria contendo todos os movimentos executados pelo Administrador e a disponibilização de relatórios periódicos (semanais, por exemplo) para que sejam formalmente revisados.

Por analogia com um destacamento militar, é como se o Administrador pudesse “nomear” um “soldado” (com pouco poder de acesso às informações) em um “general” (com poder total de acesso) e vice-versa. Inclusive, pode “se nomear” como o “general”. Se assim o fizer, sem qualquer rastro de suas atividades, não existirá qualquer controle na área da segurança da informação. Igualmente, se houver o registro das atividades e não houver o adequado monitoramento, o processo de segurança continuará totalmente falho.

2.4 Usuário e Indivíduo – uma relação que pode ser conflituosa

Um usuário é qualquer indivíduo que, por necessidade de negócios, precise do acesso ao “SAN”. O acesso pode ter diversos poderes, tais como: somente leitura, leitura e atualização, inclusão e/ou eliminar (“deletar”), etc.

Entretanto, um mesmo indivíduo pode ter diversos “identificadores de usuário” sob seu nome, isto é, ter vários “*user-ids*” nos diversos ambientes computacionais de uma empresa. Muitas vezes, esta ocorrência não é percebida pelos gestores, o que dificulta e/ou impede uma correta análise de riscos nos casos de acúmulo indesejável de poderes. Por isto, alguns cuidados são fundamentais para um controle eficiente.

Sempre que um usuário tiver a necessidade de acesso a um sistema, o requerimento deve ser feito pelo seu gestor ao proprietário do “SAN”. Esta etapa representa a aprovação prévia do seu superior. Ainda que o superior seja o próprio proprietário, é obrigatória a aprovação formal do gestor.

O requerimento deve conter uma definição clara dos atributos do acesso, com as respectivas justificativas, isto é, a real “necessidade de negócio” (em inglês, “*business need*”).

Existem casos em que uma pessoa que trabalha em uma área (exemplo: Contas a Receber), precise acessar o sistema de outra área (por exemplo, a Contabilidade). Então, cabe aos gestores, incluindo os Proprietários, a avaliação conjunta do pedido de acesso. Após aprovado, o pedido é enviado ao Administrador de Segurança do “SAN” considerado para que seja providenciada a concessão do acesso aprovado.

2.5 Perfil do Usuário

Conjunto de poderes de acesso que um usuário precisa possuir para desenvolver suas atividades na empresa. Algumas empresas confeccionam diversos “perfis” relacionando-os aos cargos e/ou funções na empresa, em concordância com as áreas de negócio e o departamento de Recursos Humanos.

Citamos como exemplo, a área de Compras: existem poderes de acesso diferentes dependendo da função: Comprador “Junior” (menos poderes), Comprador *“Senior”* (mais poderes), etc. Assim, quando um indivíduo assume uma função na empresa, o gestor já sabe qual é o perfil que melhor se adéqua para o exercício de suas atividades.

Mais uma vez, é importante ter cuidado com a relação “usuário – indivíduo”, a fim de que uma mesma pessoa com mais de um “*user-id*” seja convenientemente avaliado em relação aos seus poderes acumulados de acesso.

É comum haver analistas de sistemas, técnicos da área de “TIC” da empresa ou do fornecedor do “SAN” com acessos indevidos ao “SAN” sem justificativa da necessidade de negócios. Ainda que surja um problema no “SAN” que obrigue a intervenção de um profissional técnico, é imprescindível que o acesso concedido seja somente de “leitura”, por

um período de tempo limitado à resolução do problema. Durante o tempo de acesso, as atividades devem ser totalmente monitoradas por outra pessoa da área de negócios.

2.6 Separação de Responsabilidades

Uma solicitação de acesso deve ser avaliada em conjunto com outros acessos já concedidos a um mesmo indivíduo e/ou que estão sendo pleiteados naquele momento. Denominamos este cuidado como o princípio a ser seguido pelos gestores de um "SAN" logo após a avaliação da "necessidade de negócios": a avaliação com foco na segregação de funções ou "separação de responsabilidades".

O objetivo é identificar possíveis acúmulos indesejados de poder em uma mesma pessoa. Se o conjunto dos acessos for imprescindível, ainda que avaliada como perigosa, é imperioso que a aprovação dos acessos só deva ser concedida mediante a avaliação dos gestores e diretores das linhas gerenciais envolvidas, devidamente aprovadas nos níveis competentes e com o estabelecimento de ações disciplinadoras conforme a seguir:

- **Ações mitigadoras – para minimizar ou eliminar riscos. Exemplos:**
  - Um estagiário da área de compras precisa efetivar compras visto que há carência de profissionais no setor e as normas da empresa dificultam esta prática. O acesso poderá ser concedido, provisoriamente, com a condição de que as transações de compras oriundas do estagiário estejam com valores menores do que um limite máximo estabelecido e, ainda assim, sob a supervisão de um comprador efetivo.
  - O Administrador de Segurança do "SAN" precisa também de acesso para atualizar informações constantes no próprio sistema em que é administrador, no caso, o "Contas a Receber". Deste modo, além do poder privilegiado de alterar outros usuários com poderes diferenciados, ainda poderá alterar dados financeiros de negócios. Neste caso, o acesso ao "SAN" poderá ser concedido mediante um limite do poder de acesso: somente poderá atualizar informações em um grupo restrito de "clientes" e/ou em determinadas "faturas em aberto".
- **Medidas Compensatórias – para minimizar ou eliminar vulnerabilidades. Exemplos:**

- No exemplo anterior do estagiário, a compensação se refere a que todas as compras feitas pelo estagiário serão aprovadas *"a posteriori*" por um comprador sênior da organização e um resumo semanal das compras será avaliada pelo conjunto de transações realizadas no período.
- No caso do Administrador de Segurança, o acesso poderá ser concedido mediante a gravação de registros de cada transação efetivada por ele, de tal modo que permita o monitoramento e avaliação de todas as alterações realizadas durante um período.

2.7 Avaliação e Aceitação de Risco

É o processo de identificação, análise e avaliação das vulnerabilidades e riscos de cada processo de negócio e os impactos na empresa. É uma ferramenta de gestão e não um mero item no planejamento da segurança.

A identificação e avaliação dos riscos em função do impacto no negócio são essenciais na determinação de quais controles são necessários e do nível de investimento.

O ponto inicial do ciclo de gerência dos riscos é a compreensão dos riscos do ambiente associados com a segurança da informação. Deste modo, as seguintes atividades são importantes no processo de Gestão de Riscos:

- Reconhecer os recursos de informação como ativos vitais para a organização.
- Identificar os ativos de segurança da informação e determinar sua propriedade.
- Assegurar que os proprietários recebam orientação adequada sobre suas responsabilidades.
- Desenvolver procedimentos práticos para análise de risco que associem a segurança às necessidades da organização.
- Gerenciar continuamente os riscos.

Deve detalhar as etapas do processo e explicar claramente o tratamento a ser dado ao risco (minimizar, eliminar, aceitar ou transferir) e o plano de ação, com o cronograma das atividades necessárias para cumprir o objetivo do tratamento que foi selecionado e aprovado.

O cronograma deve conter, obrigatoriamente, para cada atividade, o relacionamento com a completude de atividades precedentes, datas compromissadas para conclusão e os respectivos responsáveis.

O processo de Avaliação / Aceitação deve prever um limite razoável de validade para garantir a execução das atividades tempestivamente e evitar postergações duradouras e indesejadas.

Nos exemplos citados anteriormente, seria a definição de um parâmetro de validade do processo, como por exemplo, seis meses. Ainda sobre os exemplos anteriores, o processo teria como objetivo a “efetivação do estagiário de Compras” e “a admissão de mais um colaborador no Contas a Receber”, ambos no prazo de 6 meses.

O processo também deve considerar a hipótese de nova avaliação após o prazo definido na política da empresa a fim de possibilitar um diferimento, desde que justificado. Por exemplo: ao término da primeira avaliação, a postergação para mais seis meses. Para evitar adiamentos sucessivos, o processo deve determinar uma quantidade bem pequena de possíveis prorrogações.

2.8 Trilhas de Auditoria

É o mecanismo essencial e básico para permitir rastreamento de operações realizadas via sistemas. É muito diferente do “log” de suporte técnico, pois este registra todas as operações fundamentais de um processo tecnológico, com registros enormes, sem o foco adequado ao negócio.

Cada proprietário de um “SAN” deve definir as transações consideradas como sensíveis ao seu negócio. Normalmente são as que alteram dados financeiros e/ou possam influir nos resultados financeiros de uma empresa.

Assim, por exemplo, as transações de atualização de um Controle de Estoque podem influir no valor do ativo armazenado em um local. Da mesma maneira, as baixas de faturas vencidas em um departamento de Contas a Receber, influem no valor pendente de recebimento por parte de clientes devedores. Por outro lado, a modificação de um endereço de um colaborador certamente não influencia o resultado financeiro da empresa. Deste modo, é importante a definição dos eventos que deverão ser passíveis de um rastreamento, isto é, definir o caminho de retorno a partir de um resultado obtido de um “SAN”. Estes eventos são as transações sensíveis.

Conhecidas as transações, a composição da trilha deve ser definida. Normalmente bastam poucas informações, tais como: “*user-id*” responsável pela transação, código da transação, data e hora (completos) do evento, a informação anterior e a atual.

É fundamental que as trilhas obtidas sejam protegidas contra acessos não autorizados e o acesso deve ser sempre do tipo “somente leitura” e nunca com o poder de alteração, deleção ou inclusão. Também devem ser preparados programas de facílima

linguagem (do tipo *"end-user",* disponíveis em profusão no mercado) para permitir que os gestores possam extrair relatórios de controle e monitoramento das transações sensíveis.

2.9 Cópia de segurança (*"backup"*).

Dependendo da finalidade de utilização do *"backup"*, existem dois tipos a considerar:

- ***"backup"* operacional:** necessário para reestabelecer uma posição anterior das bases de dados quando ocorre uma falha nas operações cotidianas, tais como, falta de energia, erro no sistema operacional ou no "SAN", erro na rede de teleprocessamento, etc.
- ***"backup"* vital:** cópia para prevenção em um problema de maior magnitude, desastroso, que pode impactar, ao mesmo tempo, diversos tipos de serviço por tempo indeterminado com grandes prejuízos para a organização. Para um sinistro do tipo desastre nas instalações e/ou áreas onde se situa o ambiente de tecnologia, estas cópias permitem a restauração gradual do negócio, desde que exista um Plano de Continuidade de Negócios adequado.

Em ambos os casos, é importante que o Proprietário do "SAN", juntamente com os responsáveis técnicos pelo desenvolvimento ou manutenção do "SAN", defina as bases de dados necessárias para a restauração do sistema em casos de falhas, os procedimentos de sua utilização quando necessário, a quantidade de versões anteriores a serem mantidas e o tempo de retenção delas.

As cópias de segurança devem ter o mesmo grau de confidencialidade e importância das bases de dados que originaram as cópias. Embora este trabalho não tenha o objetivo de definir e explicar detalhadamente o que é um Plano de Continuidade de Negócios e respectivos Planos de Desastres, é importante realçar o valor das cópias de segurança de um "SAN", pois é a partir da análise de sua importância para o negócio que os Gestores capacitam a sobrevivência da empresa ante uma situação intolerável que a leve à completa inoperância no mercado onde atua.

2.10 Classificação de segurança.

Sendo a informação um dos principais ativos em uma organização (a outra é o profissional colaborador) é preponderante que ela seja classificada em função de sua

importância ao negócio considerando os impactos negativos (financeiros, de imagem, legais, etc.) que podem advir na sua manipulação indevida.

A organização deve ter um processo aprovado e documentado para que todos os tipos de informação, em mídia eletrônica ou não, vindos do mundo externo ou originados internamente, sejam adequadamente classificados conforme a proteção requerida em uma determinada circunstância.

Assim, por exemplo, as informações relativas a um novo modelo de comercialização a ser lançado no mercado nos próximos meses, podem ser classificadas como “confidencial” até sua apresentação ao público. Após o lançamento o nível de classificação pode ser alterado para “uso público”.

Do mesmo modo, algumas informações financeiras de uma empresa podem ser consideradas como “uso interno” e outras como “confidenciais”.

O primeiro responsável pela definição dos níveis de classificação das informações de um “SAN” é o Proprietário. Ao corpo técnico da “TIC” cabe a implantação de procedimentos e mecanismos de segurança compatíveis com os níveis utilizados pela organização.

Os níveis de classificação utilizados pela organização devem estar aprovados, documentados e divulgados para todos os colaboradores. Também devem ser incluídos os procedimentos necessários para tratar cada um dos tipos de classificação em função do meio onde a informação está armazenada (mídia eletrônica ou não) e a atividade a ser executada (geração inicial da informação, divulgação, transmissão, eliminação, etc.).

2.11 Gerência de Mudanças.

É importante que todas as atualizações em um sistema, sejam este operacional ou aplicativo de negócios, sejam adequadamente gerenciadas pelo seu Proprietário. Pode haver inúmeras causas para estas alterações: aperfeiçoamento das funções e/ou atividades da programação / estrutura de mecanismos de controle do sistema, correção de um problema que precisa ser sanado, atualização de parâmetros para atender mudanças da legislação ou de normas internas da empresa, etc.

Deste modo, o Proprietário deve documentar todas as mudanças realizadas em seu “SAN”, assegurando que todos os processos ocorridos estão aprovados e documentados.

A documentação deve incluir, minimamente, as aprovações do Proprietário e de todos os gestores das áreas de negócio impactadas pela mudança e pelos gestores da área de Tecnologia da Informação e Comunicação da empresa (ou do fornecedor de serviços de

"TIC") que possuem sistemas envolvidos na mudança. Também devem ser arquivados a análise dos riscos da mudança, os testes previamente realizados e as aprovações relativas aos resultados após a efetivação da mudança.

Toda a documentação deve fazer parte do Manual de Funções do "SAN" (ou similar) que permita ao Proprietário conhecer todas as atualizações feitas no seu sistema ("por quê","quando", "quem", "como", análises e resultados.

2.12 Gerência de aplicações de *"Patches"* (*"Patch Management"*).

Em toda a instalação "TIC", existem diversos sistemas operacionais, tanto em ambientes *"main frame"* como em ambientes *"midi-range"* e *"micro-informática"*. Assim, por exemplo, "Windows", "Linux", "Websphere", "Tivoli", "Oracle", etc., são continuamente atualizados por seus fabricantes em termos de aperfeiçoamentos ou correção de alguma "brecha" ou problema de segurança identificado.

As urgências das alterações são definidas pelos próprios fabricantes e são denominadas como "severidade". Cabe à organização estabelecer o critério de implantação, relacionando a severidade ao tempo máximo de correção / atualização para cada tipo de ambiente.

Um exemplo mais detalhado:

Modelo de Prazos máximos de implantação do "patch":

Tabela 1: Modelo de prazos máximos de implantação do *patch - Rede*

Ambiente	Severidade	Prazo Máx. Instalação (dias)
Rede	Baixa	30
	Média	15
	Alta	7

Fonte: Elaborado pelo autor em conjunto com o orientador.

Tabela 2: Modelo de prazos máximos de implantação do patch - Outros

Ambiente	Severidade	Prazo Máx. Instalação (dias)
Outros	Baixa	60
	Média	30
	Alta	15

Fonte: Elaborado pelo autor em conjunto com o orientador.

Na tabela acima, o ambiente da rede é considerado como mais prioritário do que os demais ambientes.

Uma empresa deve estabelecer o cronograma de atualizações de “patches” considerando as suas necessidades. Por esta razão, é comum que a faixa de tempo destinada à atualização seja em um fim de semana.

Daí a importância de controlar e monitorar os resultados das atualizações dos *“patches”*, principalmente os de maior severidade e/ou os que ultrapassam o tempo previsto sem uma análise criteriosa e a definição de planos de ação para corrigir os desvios e minimizar os riscos dos atrasos.

Neste trabalho, focamos a possível dependência de um “SAN”, desenvolvido e/ou suportado por algum sistema operacional cujo fabricante divulga uma correção (*“patch”*) para seu produto.

Existem outros processos de identificação de “falhas” ou “fragilidades” nos diversos sistemas de informática de uma organização, esteja este serviço em suas próprias instalações ou em um fornecedor: Citamos como exemplos: *“Vulnerability Scan”* (pesquisa de vulnerabilidades) e “Health Check” (checagem da “saúde” da segurança).

São processos periódicos, definidos e planejados antecipadamente pela equipe técnica, cujos resultados demandam planos de ação para as devidas correções. Neste trabalho consideramos somente o *“Patch Management”* visto que o foco é em relação às áreas de negócios, especificamente ao Proprietário do “SAN”.

2.13 Política de Segurança da Informação.

Promove orientação e suporte da direção para segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes. Após aprovação da política por parte da direção da empresa, essa deve ainda atribuir funções de segurança e fazer uma análise crítica de sua implementação por toda a organização. É desejável que essa Política seja de fácil interpretação e reflita os objetivos do negócio.

As diretrizes de segurança da informação estão baseadas na Norma ABNT família ISO/IEC 27000. A seguir, as principais normas relativas ao assunto:

- **27001:** Padrão de especificação para um “SGSI” – Sistema Gerencial de Segurança da Informação.
- **27002:** Novo padrão de orientação detalhada das normas de segurança consideradas como “boas práticas”, que serão detalhadas mais adiante. É considerada como o ponto de entrada mais importante na implantação de uma Política de Segurança da Informação. Baseia-se na antiga ISO 17799.
- **27003:** Guia para a implantação do “SGSI”.

- **27004:** Padrão de medição e métricas para o “SGSI”.
- **27005:** Padrão de Gestão de Risco da Segurança da Informação.
- **27006:** Guias para organizações certificadoras de Certificação “SGSI”.

Neste trabalho, detalhamos um pouco mais a ISO/IEC 27002 que é um dos principais suportes para uma avaliação de um “SAN”.

a) **Organização da segurança da informação:** Deve haver uma estrutura de gerenciamento da segurança da informação com o objetivo de controlar e implantar a segurança da informação, incluindo os “SANs”. Assim, por exemplo, cada “SAN” deve ter um Proprietário e um Administrador de Segurança devidamente nomeado pelas áreas Diretoras da Empresa.
b) **Gestão de ativos:** Todos os ativos devem estar inventariados e possuir um responsável pela manutenção de seus controles. Embora o proprietário possa delegar a implantação ou alteração em funções de controle, ele ainda permanece responsável por sua adequada proteção. No caso dos “SAN” todas as bases de dados, programas, rotinas computacionais, identificadores de usuários, perfis de segurança, manuais, etc. devem ser identificados, classificados e convenientemente protegidos contra acessos indevidos.
c) **Recursos humanos:** Assegurar que todas as pessoas envolvidas na organização, sejam elas funcionários, fornecedores ou terceiros, entendam suas responsabilidades e atuem de acordo com suas atribuições, evitando assim possíveis fraudes e/ou desvios. As responsabilidades podem ser atribuídas antes da contratação de um funcionário. Elas devem estar listadas nas descrições de cargos. Deve haver um termo para contratação de serviços de terceiros e fornecedores. O reconhecimento dos termos e responsabilidades pode ser feito através de assinatura. A ciência por parte dos colaboradores deve ser regularmente atualizada. O Proprietário deve garantir que todos os usuários de seu “SAN” tenham dado ciência nas Normas e procedimentos da empresa quanto a Segurança da Informação.
d) **Segurança física e do ambiente:** Garantir que as instalações não estejam expostas a danos e interferências, bem como sujeitas a acessos físicos não autorizados. Esse controle é necessário porque são nos ambientes computacionais que trafegam os dados sensíveis da

organização. O Proprietário deve assegurar que as informações de negócios sejam armazenadas de acordo com a classificação de segurança definida pelo Proprietário. Caso sejam confidenciais / sigilosas, devem estar sob proteção adicional, como por exemplo, segregadas em salas-cofre e/ou em ambiente com acesso restrito. Neste caso, é preponderante a existência de controles rigorosos de acesso a estas áreas, contendo, pelo menos, os nomes dos indivíduos que acessaram o ambiente, quando, motivo, informações acessadas e a aprovação do Proprietário ou de seu preposto.

e) **Gerenciamento das operações e comunicações:** Assegurar que os recursos de processamento da informação sejam utilizados de forma correta e segura. É desejável que seja definido um responsável pela gestão e operação desses recursos. Isto pode ser feito através do desenvolvimento de procedimentos operacionais. Dentre os procedimentos estão incluídos a segregação de funções e áreas; o monitoramento e análise crítica de serviços terceirizados; o planejamento e o processo de aceitação dos sistemas; a proteção contra códigos maliciosos e códigos móveis; a geração de cópias de segurança; gerenciamento da segurança em redes; o manuseio, controle e proteção das mídias; a troca de informações entre organizações e internamente; e o monitoramento, o registro e a auditoria. Inclui-se neste gerenciamento o controle de "*Patch Management*" (vide 2.12) que objetiva a adequada e correta implantação de correções e/ou atualizações nos diversos sistemas operacionais de uma rede e/ou instalação de informática.

f) **Controle de acesso:** O acesso à informação, bem como os seus recursos de processamento e processos de negócio devem ser controlados através do requisito de negócios e segurança da informação. Isso inclui a política de controle de acesso; o registro dos usuários; o gerenciamento de privilégios; a concessão de senhas; a análise crítica dos direitos de acesso; a seleção e uso adequado de senhas; o controle de acesso à rede; o controle de acesso ao sistema operacional, o controle de acesso à aplicação e à informação; e o controle do uso da computação móvel e dos recursos de trabalho remoto. O Proprietário deve garantir que todos os usuários de seu "SAN" tenham seus acessos aprovados por ele (e, em alguns casos pelo gestor do usuário, caso este esteja em outra área da empresa), recertificado em bases regulares e

que estejam cientes das normas e procedimentos da empresa quanto à divulgação indevida de informações.

g) **Aquisição, desenvolvimento e manutenção de sistemas de informação:** As necessidades de segurança dos sistemas de informação precisam ser levadas em conta em projetos de implantação. Isso quer dizer que os requisitos de segurança dos sistemas operacionais, infraestrutura, aplicações de negócio, produtos de prateleira (*softwares* desenvolvidos por "*softhouses*"), serviços e aplicações desenvolvidas pelo usuário sejam definidos e justificados na fase inicial de um projeto.

h) **Gestão de incidentes de segurança da informação:** Assegurar que os incidentes relacionados à segurança da informação sejam comunicados de forma tempestiva, para que seja corrigido o quanto antes aconteçam. Os funcionários, fornecedores e terceiros devem seguir procedimentos preestabelecidos para reportar fragilidades aos responsáveis a fim de adotarem-se medidas para resolução do problema.

i) **Gestão da continuidade do negócio:** Garantir a continuidade do negócio através da proteção dos processos críticos, no caso de interrupções, o sistema deve ser reestabelecido em tempo hábil. Esse processo minimiza o impacto dos incidentes na organização, que podem ser ocasionados por desastres naturais, acidentes, falta de equipamentos e ações intencionais e ajuda a medir o impacto de sua ocorrência na organização.

j) **Conformidade:** Garantir que não sejam violadas quaisquer obrigações legais, estatutárias, regulamentares ou contratuais referentes à segurança da informação. É desejável o uso de consultoria especializada para atender às regulamentações impostas aos dados computacionais.

Um dos itens mais importantes e mais esquecidos e/ou negligenciados pelos proprietários de "SAN"s e pelos gestores da área de "TIC" é o monitoramento dos "SLA"s – *Service Level Agreement"* ou Acordos de Nível de Serviço. Por este motivo, os detalharemos mais adiante no item específico: "SLM" – *Service Level Management*" que é o monitoramento conjunto de todos os "SLA"s de uma determinada área de atuação.

2.14 Gestão da Segurança da Informação.

A norma utilizada para auxiliar uma organização na implantação de um Sistema de Gestão da Segurança da Informação – "SGSI", é a ISO IEC 27001 (que substituiu a norma britânica BS 7799-2:2002).

Ela especifica os requisitos de controles de segurança da informação necessários para estabelecer, implantar, operar, monitorar, analisar criticamente, manter e melhorar um sistema de gestão documentado dentro do contexto dos riscos de negócio da organização.

Para a melhor gestão da segurança da informação, é necessária a implantação de um conjunto de técnicas, mecanismos e metodologias que permitam, em tempo hábil, a identificação dos riscos e os controles necessários para o adequado tratamento de cada um deles, além de garantir que as informações corporativas estejam disponíveis, íntegras e protegidas. As principais etapas do conjunto são as seguintes:

a) **Estabelecimento do grupo central do "SGSI":** O "SGSI" deve ser constituído por um grupo que atue como o seu comando central a fim de assegurar maior eficácia e eficiência na identificação e tratamento dos riscos das operações computacionais relacionadas aos negócios, além da melhor utilização dos recursos disponíveis. Este grupo deve assessorar todas as unidades / setores da organização atuando como facilitador e canal de informação para alta gerência / diretoria, além de supervisionar todo o "SGSI". Na maioria das empresas, o coordenador central do "SGSI" pertence à equipe da Segurança da Informação, através da figura do "CSO" (*"Chief Security Officer"*), ou Supervisor / Superintendente da Segurança da Informação na empresa. Dentre suas responsabilidades, destacamos:

   - Desenvolver, manter, divulgar e esclarecer as políticas e diretrizes globais da organização em relação à segurança da informação.
   - Implantar e manter a Política de Segurança da Informação - "PSI".
   - Ser o ponto focal para esclarecimento das dúvidas e orientação acerca da "PSI". Educar gestores e usuários acerca dos riscos de segurança da informação.
   - Esclarecer ao corpo diretor as implicações de segurança no uso de novas tecnologias.
   - Pesquisar acerca de novas ameaças, vulnerabilidades e técnicas de controle.

- Testar controles, registrar incidentes e avaliar conformidade com políticas.
- Estabelecer grupo de resposta a incidentes.
- Definir a classificação das informações.
- Manter um canal de comunicação com a alta gerência para esclarecer detalhes que permitam maior compreensão dos riscos.
- Estimular a capacitação dos administradores de sistemas, pois compõem a primeira linha de defesa da organização, principalmente pelo poder a eles conferido de efetivar as concessões de acesso aos dados de negócio.

b) Estrutura do "SGSI": Deve haver uma clara distinção entre política, diretriz e procedimentos: A Política deve sintetizar os requisitos imperativos e essenciais, o que facilita sua aprovação e revisão. O "SGSI" deve estar fundamentado em uma política que leve em consideração os requerimentos de negócios, as estratégias da empresa, os objetivos de curto, médio e longo prazo e a utilização de metodologias consagradas pelo mercado como as melhores práticas na área de segurança da informação. O conjunto destes atributos direciona a elaboração e manutenção da política como um todo. Especificamente quanto à "PSI", trata-se de um dos componentes do "SGSI" e não o seu todo. Assim, por exemplo, o "SGSI" contém outros componentes, tais como o processo de monitoramento, os indicadores de metas e de desempenho, as avaliações periódicas, as estruturas de contingência e plano de desastre. Em uma organização a Política – "PSI" – deve resumir os tópicos relacionados com a segurança da informação com as informações genéricas de cada assunto. A orientação e direcionamento da Política, bem como explicações mais completas devem constar das "Diretrizes". As minúcias detalhadas, incluindo os roteiros do "passo a passo" devem ser explicadas minuciosamente nos "Procedimentos". Consideremos como exemplo, o assunto "Classificação da Informação":

- A Política "PSI" deve definir de forma abrangente: "Toda a informação corporativa deve ser adequadamente classificada pelo Proprietário da Informação, conforme as regras vigentes".
- A "Diretriz" fornece uma explicação mais detalhada: Os níveis de classificação da informação utilizados pela empresa, considerando do menor para o maior risco são: "uso geral" "uso

interno", "uso restrito", "confidencial" e "secreto". O Proprietário da informação é o responsável pela sua avaliação adequada, considerando os riscos financeiros, operacionais, jurídicos e legais envolvidos em eventual uso inadequado.

- O "Procedimento" contém o *"modus operandi"* – regras, detalhes, passo a passo, tabelas, anexos, etc. relacionados à Classificação da Segurança: "As tabelas "X" e "Y", mostram os parâmetros utilizados na empresa para dimensionar os riscos financeiros, operacionais, jurídicos e legais, considerando que o maior nível de um deles define o nível de classificação da segurança. Qualquer dúvida, submeter à apreciação à sua linha gerencial / diretora ou ao Coordenador de Segurança da sua área de negócio". "As tabelas "A" (armazenamento em mídia magnética) e "B" (armazenamento em mídia NÃO magnética) explicam, para cada tipo de ação (cópia, divulgação, eliminação, transporte, transmissão, etc.), o procedimento e comportamento esperado de cada usuário. Desvios às normas e procedimentos serão passíveis de penalidades". (As tabelas constituem Anexos aos Procedimentos).

O objetivo é que a "Política" propriamente dita seja uma "constituição" e a maioria das atualizações seja feita nos "Procedimentos" ou nas "Diretrizes". Deste modo, as alterações e aperfeiçoamentos serão mais ágeis e eficazes.

- Monitoramento e avaliação das Políticas e Controles: O "SGSI" prevê o monitoramento das atividades previstas na "PCI" e avaliação da eficácia dos seus controles. As principais diretrizes são as seguintes:
  - Monitoramento de fatores essenciais que podem aumentar riscos, tais como o nível de conscientização do pessoal e o acompanhamento da evolução ou não de incidentes.
  - Teste da eficácia dos controles, realizado por revisores internos e auditorias, considerando obrigatoriamente os testes de invasão, simulação de desastres e indisponibilidades de sistema aplicativo de negócio – "SAN" e do local de trabalho (perda das estações de trabalho e/ou impossibilidade de acesso ao ambiente de trabalho).
  - Registro e análise de incidentes de segurança.

- Revisão e aperfeiçoamento das políticas, práticas e controles existentes.
- Avaliação de novas técnicas de segurança, ferramentas e mecanismos de gestão.

c) Posicionamento do "SGSI": A tendência das grandes organizações é posicionar a "SGSI" e respectiva política sob uma organização mais ampla, denominada "Gestão de Riscos", bem como posicionar o Plano de Recuperação de Desastre sob uma Política de Continuidade de Negócios (o mais correto). Adicionalmente, a Continuidade de Negócios também deve abranger planos de contingência, não somente para casos de desastre, mas também para outros tipos de cenários, tais como a indisponibilidade de um sistema aplicativo (ex.: mau funcionamento, situação imprevista), a indisponibilidade do local de trabalho (ex: greve, tempestade) e outros cenários devidamente mapeados por um processo de avaliação de riscos.

2.15 Acordo de Níveis de Serviço – Gestão

2.15.1 Introdução

Toda contratação de serviços, principalmente na área de informática, deve inserir nas suas cláusulas, as especificações dos níveis de serviços esperados pela contratante conforme as condições possíveis da contratada. Estes níveis de serviços acordados entre as partes são conhecidos como "Acordos de Níveis de Serviço" ou pela sua sigla em inglês "SLA" (*"Service Level Agreement"*).

Para gerenciar estes Acordos, é preciso que exista um processo de definição de medidas, a medição propriamente dita, a captura das informações medidas e o monitoramento do processo para permitir avaliações constantes sobre os resultados esperados.

Focando no tema de nosso trabalho – um aplicativo de negócio – o "SAN", é primordial que se identifique os requisitos importantes da área de negócio que o "SAN" vai atender. Os "envolvidos" e "interessados" pelo serviço - normalmente os usuários finais da empresa e o Proprietário do "SAN" - devem influir na definição dos parâmetros junto com o fornecedor dos serviços, compreender os ambientes em que o sistema é processado, concordar com os parâmetros e formas de medição e, finalmente, acompanhar e avaliar os resultados.

O “SLM” – “*Service Level Management*” – Gestão dos Níveis de Serviços é o conjunto integrado de medições dos diversos “SLA”s de um ambiente de negócios. Essa gestão exige o uso de ferramentas de software, o cronograma de medições e o estudo analítico das variáveis que podem influir nos resultados a fim de incidentes e problemas de outras áreas não impactem os resultados de um “SLA”. Deste modo, por exemplo, a duração da falta de energia em um ambiente de “TIC” não deve influir negativamente na medição do tempo de resposta de um serviço do tipo “SAN” que depende de serviços “online”. Por outro lado, devem existir “SLA”s específicos em relação ao suprimento de energia pela concessionária local.

Considerando um “SAN”s, um “SLA” típico deve incluir processos de medição sobre os registros de aberturas de chamados na área denominada como *"help-desk"* (suporte de primeiro nível de incidentes), tempos de paralisação de serviços e/ou equipamentos e outros eventos que tornam o serviço temporariamente indisponível, o tempo de resposta no ambiente “online”, qualidade de testes (abrangência, profundidade, documentação, etc.) além de aspectos relacionados à garantia da continuidade do contrato para evitar conflitos entre as partes. Por isto, incluem-se medições relacionadas ao nível de satisfação da contratante com a contratada e a qualidade do gerenciamento de todo o serviço.

Resumindo, os Acordos de Níveis de Serviço constituem poderosas ferramentas para controle e monitoramento dos serviços executados por um fornecedor, seja este interno ou externo. Todas as empresas, públicas ou privadas, de pequeno, médio ou grande porte, devem possuir processos gerenciais para acompanhar os resultados, quantificados e qualificados, dos serviços executados ao longo de um período. As informações coletadas devem, então, ser comparadas com os valores compromissados formalmente nos contratos e devem ser adequadamente avaliados considerando eventuais incidentes ocorridos em outras áreas, filtrando, deste modo, a qualidade do resultado.

Se estes resultados forem insatisfatórios em relação ao esperado e devidos a problemas de desempenho do fornecedor, devem existir cláusulas contratuais para ações punitivas e/ou ressarcimento, tais como: multas, descontos e até mesmo o cancelamento do contrato. As penalidades podem ser definidas isoladamente (um tipo para cada resultado insatisfatório) ou no conjunto (um tipo para a resultante negativa de diversos resultados sejam estes individualmente positivos ou não).

2.15.2 Parâmetros principais (com foco nos Sistemas Aplicativos de Negócios – “SAN”):

- **Tempo Médio entre Falhas (“MTBF” – *Mean Time Between Failures*):**
  É o tempo médio entre interrupções de serviço. No caso do “SAN”,

considera-se como interrupção qualquer incidente inesperado no funcionamento do software aplicativo. Exemplo: o “SLA” estabelece um “MTBF” de 6 meses. Isto é, admite-se apenas uma falha do aplicativo a cada 6 meses. Deve haver uma tabela para especificar o percentual do “SLA” para maior quantidade de falhas no período considerado. Um exemplo de “MTBF” em um “SAN” para um período de seis meses:

Tabela 3: Modelo de MTBF

Interrupções devidas ao “SAN”	Percentual do “SLA”
1	100%
2	90%
3	80%
Etc.	

Fonte: Elaborado pelo autor em conjunto com o orientador.

- **Tempo Médio de Reparo (MTTSR” – *“Mean Time To Service Repair”*):** Refere-se ao tempo médio para reparo de um componente ou serviço. Esse parâmetro associado ao anterior “MTBF” mede a eficiência do reparo de um componente ou serviço. Note que não basta reparar o componente rapidamente se este apresenta constantes problemas de interrupção. Continuando com o exemplo de um “SAN”, é preciso medir também o desempenho do suporte para este tipo de incidente. Assim por exemplo, poderia ser definido que, para falhas no software aplicativo – “SAN”, a solução deve ser encontrada e efetivada em um período máximo de 6 horas. Pode ser estabelecida uma tabela de nível de atendimento de “SLA” em função das horas necessárias para a correção de um problema específico no “SAN”. Não se incluem problemas de algum sistema operacional ou da rede. No exemplo, estamos nos atendo somente aos incidentes do “SAN”. Um exemplo de atendimento de “SLA” para o Tempo Médio de Reparo em um “SAN”:

Tabela 4: Modelo de Acordo de um SLA

Tempo decorrido para a solução	Percentual do “SLA”
Até 6 horas	100%
De 6,01 horas até 8 horas	90%
De 8,01 horas até 10 horas	80%
Etc.	

Fonte: Elaborado pelo autor em conjunto com o orientador.

As tabelas dos itens 1 e 2 anteriores podem ser consideradas pela resultante entre elas a fim de aperfeiçoar a avaliação do fornecedor. Assim, por exemplo, se ocorreram 2 incidentes com durações de reparo iguais a 5 horas e 10 horas, o resultado do primeiro item é 90% (2 incidentes). Em relação à segunda tabela, um dos incidentes tem o percentual de 80% e o outro, de 100%. A resultante dos dois itens seria: 0,9 x 1 x 0,8 = 0,72. Se o contrato estabelece um mínimo de90% para os dois itens em conjunto, o fornecedor, pelo exemplo, não atingiu o "SLA" esperado.

2.15.3 Disponibilidade:

Mede a disponibilidade total do serviço contratado considerando um período do dia, podendo, também, levar em conta os "horários de pico durante o dia e durante o final do mês", etc. Na maioria das vezes os contratos de prestação de serviço são direcionados para atender à operação 24x7x365, isto é, 24 horas por dia, sete dias da semana e durante todos os dias do ano. Entretanto, há necessidade de algumas interrupções para manutenções de serviços (aperfeiçoamento do HW e/ou SW, melhoramentos na rede, correções para eliminar vulnerabilidades, etc.). Por esta razão, os "SLA"s devem prever estas intervenções de modo que as medições sejam ajustadas criteriosa e adequadamente. Exemplificando: um "SAN" deve estar disponível para o ambiente "online" durante o período de 6h às 21h todos os dias úteis para todo o País, com tempo médio de resposta igual ou menor que 3 segundos. Fora destes períodos, admite-se um tempo de resposta igual ou menor que 5 segundos. Neste caso não são considerados os incidentes da rede e sim do "SAN". Por este motivo, as medições devem ser ajustadas caso sejam verificados problemas com a rede empresarial. Do mesmo modo que os dois primeiros itens, o contrato deve incluir tabelas de correspondência de "resultados obtidos durante as medições" em relação ao esperado e os percentuais de "SLA" que serão considerados.

2.15.4 Documentação:

Mede o nível de atualização da documentação e o que foi acordado no contrato. É vital possuir uma documentação atualizada para assegurar soluções eficazes e rápidas em qualquer incidente, evitando descontinuidade dos serviços. Exemplo: Inspeções periódicas e aleatórias nos manuais do "SAN" e verificar a qualidade das informações e a quantidade de itens desatualizados.

2.15.5 Desempenho do "Help-desk" (suporte de primeiro nível)

Representa uma média ponderada de outros parâmetros, tais como:

- Atendimento das chamadas telefônicas até o nº toque do telefone;
- Tempo de resolução de incidentes e/ou problemas;
- Percentual de solução de incidentes e/ou problemas pelo telefone;

O primeiro parâmetro depende de um sistema telefônico especial, conhecido como DAC – Distribuidor Automático de Chamadas, que mede automaticamente o desempenho dos atendentes. Os outros parâmetros são medidos pelo sistema que controla a abertura e fechamento dos "tickets" de chamada.

2.15.6 Pesquisa de Satisfação dos Interessados / Envolvidos

Elaborada conjuntamente entre contratada e contratante, deve identificar o nível de satisfação dos usuários do serviço. No nosso foco, um "SAN", deve prever questões relacionadas ao Proprietário, ao Administrador de Segurança, aos usuários e os setores de negócio que recebem informações do "SAN". Embora o mercado defina como boa prática a pesquisa em bases anuais, é importante que os períodos sejam menores, caso se identifiquem resultados insatisfatórios. Neste caso, devem ser estabelecidos planos de ação e uma nova pesquisa deve ser executada para verificar se houve progresso ou não.

Exemplo: A pesquisa deve ter um resultado acima de 90% como "satisfeitos" ou "muito satisfeitos". Para resultados menores, deve haver uma tabela decrescente de níveis de "SLA" conforme exemplificado nos itens anteriores. A pesquisa deve ser objetiva, sem deixar margem à interpretação pelos usuários. Dependendo da negociação entre as empresas, as perguntas da pesquisa podem ter pesos diferenciados para melhor avaliar o nível de serviço.

Os parâmetros primordiais, principalmente no início das negociações para implantação e manutenção dos Sistemas Aplicativos de Negócios – "SAN"s são:

- Devem ser formalizados os seguintes parâmetros:
- Condições de negociação, incluindo prováveis futuras versões do produto.
- Prazo de instalação.
- Multas para caso de atrasos se estes forem devidos ao fornecedor.
- Custos de cada uma das etapas e tipos de serviço.
- Qualidade e suficiência dos manuais de suporte ao "SAN"
- Parâmetros e tipos de medição a serem observados para o "SLA".
- Processo de medição (ferramentas, períodos, etc.).

- Penalidades nos casos de não observância do “SLA”.
- Quantidade e qualidade dos testes (devem ser exaustivos e abrangentes).
- Tempos esperados de processamento, incluindo tarefas relacionadas à logística.
- Tempo de atendimento às manutenções excepcionais (suporte a problemas inesperados e/ou erros).
- Modalidade de negociação nos casos de interrupção das atividades do fornecedor ou de aquisição por outro fornecedor. (principalmente em relação aos “programas-fonte” do aplicativo).

Uma das técnicas mais eficazes de revisar ou auditar um “SAN” do ponto de vista do Proprietário é verificar se existe ou não “SLA”s, entre o fornecedor (seja este interno ou externo) e o Proprietário. Ainda que exista, deve ser verificado se os itens considerados são adequadamente medidos e comparados com os resultados esperados.

Em uma análise mais profunda, se são medidos e comparados, se existem providências (planos de ação com atividades, datas compromissadas e responsáveis) para os resultados insatisfatórios e se os contratos especificam penalidades que estão sendo consideradas.

Concluindo, o “SLA” é uma excelente forma de contratar serviços, pois estabelece os parâmetros que devem ser atingidos pelo provedor de serviços. Porém, os contratos baseados em “SLA” devem ter um gerenciamento eficiente para evitar perdas e desgaste no relacionamento entre a contratante e a contratada.

2.15.7 Continuidade de Negócios

As melhores práticas são definidas pelo Instituto de Continuidade de Negócios (“BCI” –*“Business Continuity Institute”*).

O Plano de Continuidade de Negócios (“PCN”), o qual é a tradução de *“Business Continuity Plan”* (“BCP”), é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre e/ou indisponibilidade dos recursos, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual ela faz parte. Além disso, sob o ponto de vista do “PCN”, o funcionamento de uma empresa deve-se a duas variáveis: os componentes e os processos.

Os componentes são todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática, infraestrutura, pessoas. Todas elas podem ser substituídas ou restauradas, de acordo com suas características.

Já os processos são as atividades realizadas para operar os negócios da empresa. Um “SAN” é um dos componentes de um processo. Assim, por exemplo, no Processo de Contas a Receber, o sistema aplicativo do negócio é a ferramenta informatizada que visa agilizar e possibilitar o adequado monitoramento das diversas etapas do processo.

O Plano de Continuidade de Negócios é constituído pelos seguintes planos:

- Plano de Administração de Crises (“PAC”);
- Plano de Recuperação de Desastres (“PRD”);
- Plano de Continuidade Operacional (“PCO”).

Todos estes planos têm como objetivo principal a formalização de ações a serem tomadas para que, em momentos de crise, a recuperação, a continuidade e a retomada possam ser efetivas, evitando que os processos críticos de negócio da organização sejam afetados, o que pode acarretar em perdas financeiras.

No que diz respeito à necessidade de atualizações, o “PCN” deve ser revisado periodicamente, pois mudanças significativas em componentes, atividades ou processos críticos de negócio podem fazer com que novas estratégias e planos de ação sejam previstos, evitando assim com que eventuais desastres desestabilizem profundamente o andamento regular do negócio da empresa.

Desastre pode ser entendido como qualquer situação que afete os processos críticos do negócio de uma organização. Consequentemente, algumas ocorrências podem ser caracterizadas como sendo desastres para uma determinada empresa, mas podem não ser caracterizadas como um desastre para outra empresa.

Neste trabalho, com foco nos “SAN”s, consideramos os processos de Gestão de Riscos, Recuperação de Desastre, Segurança e Gestão de Crises.

3. Metodologia

A pesquisa realizada caracteriza-se por descritiva dada sua finalidade e método aplicado.

Para os procedimentos empregados na realização dos estudos, utilizou-se de pesquisa bibliográfica que se deu através de consulta a livros, material disponível na internet e periódicos que tratam do assunto.

Além da pesquisa bibliográfica utilizou-se a elaboração de pesquisa de campo, onde foram entrevistados oito gestores de departamento de tecnologia da informação com o conhecimento suficiente para responder às questões, apuraram-se as suas percepções quanto aos ativos computacionais e a sua importância para a empresa. O critério utilizado para a seleção das empresas foi que essas deviam pertencer ao ramo da construção civil.

O instrumento utilizado na coleta de dados foi um formulário contendo 9 (nove) perguntas fechadas aplicadas aos respondentes que consta no anexo I deste trabalho.

4. Apresentação e Análise dos Resultados

4.1 Questionário Aplicado

Nesse item inserimos as perguntas que direcionaram nossa pesquisa. Essas estão listadas no Apêndice A e foram aplicadas a oito empresas do ramo de construção civil. As perguntas foram elaboradas baseadas na necessidade de identificar o nível de maturidade das empresas quanto à necessidade de se realizar auditorias nos processos e sistemas que garantissem conformidade de dados.

Perguntas: (em vez de “TIC”, usamos a sigla “TI”, para facilitar os respondentes, não acostumados com a sigla mais moderna).

4.2 Análise dos dados do questionário

As respostas obtidas pelas empresas ao questionário do item abaixo foram analisadas e tabuladas. Como se trata de um levantamento pode ser que as respostas tendam a ser favoráveis à situação. Caso seja realizada uma auditoria verdadeira e eficaz, possivelmente seriam encontradas inúmeras discordâncias entre as respostas obtidas e o que realmente ocorre. Algumas conclusões importantes sobre as respostas:

Admitindo-se que somente 50% das empresas pesquisadas possuem Auditoria Interna (primeiro gráfico), e que dessas, 63% existe alguém especializado em “TIC” (segundo gráfico), podemos admitir que em 32% dos casos (50% x 63% = 31,5%) existe um profissional apto verificar o estado de controle em “TIC”, em termos de auditagem e/ou para acompanhar os Auditores Externos nas suas análises.

Se 75% das empresas não possui Auditoria Externa (terceiro gráfico) e 38% não tem especialistas internos para acompanhar as revisões destas Auditorias (quarto gráfico), possivelmente não há acompanhamento dos resultados das Auditorias em 28% delas (75% x 38% = 28,50%). A falta de uma Auditoria Externa poderia ser suprida pela Auditoria Interna, contudo metade das empresas não possui esse tipo de Auditoria (e, provavelmente, nem revisões técnicas internas).

Na melhor das hipóteses, 25% não possui qualquer tipo de auditoria (quadros “1” e “3”). Entretanto, não pode ser afirmado que toda a empresa que possui Auditoria Externa, tenha também Auditoria Interna.

Todas as empresas possuem políticas, mas em 63% delas não há atualização anual da Política, sendo assim elas não refletem a situação atual das organizações, uma vez que a tecnologia, ameaças, vulnerabilidades e riscos crescem exponencialmente durante o decorrer de um ano.

Constatamos que 88% das empresas têm como comprovar que as concessões de acesso aos sistemas foram autorizadas por algum superior, mas 63% desses acessos não são revisados. Identificamos ainda que em 25% dos casos não existe uma checagem das aprovações dos acessos.

As questões aplicadas juntamente com os percentuais dos resultados podem ser vistos no Apêndice A.

5. Considerações Finais

Por algum tempo as empresas podem até conseguir prosperar sem se preocupar com as suas práticas de gestão de "TIC", mas a cada dia, a necessidade desta governança assume uma importância cada vez maior e se torna a base dos processos empresariais e o principal instrumento de implantação de estratégias corporativas.

O crescimento das empresas traz consigo a necessidade de melhoria das práticas de governança corporativa, que precisam ser suportadas por melhores práticas de governança de "TIC". Além disso, o ambiente de tecnologia vem se tornando cada vez mais complexo e dinâmico, o que dificulta seu gerenciamento, principalmente com o advento de práticas e processos relacionados ao "BYOD" (*"Bring Your Own Device"* – Traga seu próprio Dispositivo), à computação em nuvem *("Cloud Computing")* e o uso cada vez mais frequente de Redes Sociais nas empresas. Daí a importância de se desenvolver mecanismos visando a proposição de ações que elevem o nível de maturidade dos processos de "TIC" e viabilizem a boa governança dos seus ativos.

Como modelo de referência, esse trabalho propõe às tabelas mostradas nos quadros "1" a "5".

É importante ressaltar que o presente trabalho não é um manual de auditoria, uma vez que esse tema é muito mais amplo e profundo além de ser extremamente dinâmico. Sendo assim, seu objetivo é servir de instrumento metodológico contendo diretrizes básicas para realização de auditoria de sistemas de informação na área de negócios, sob o foco do gestor do aplicativo. O mesmo está aberto a mais contribuições no sentido de enriquecê-lo, principalmente nos tópicos que foram apenas exemplificados para que o leitor pudesse entender melhor o tema.

Convidamos todos os interessados para que meditem sobre o tema, aperfeiçoem, ampliem os questionários sugeridos para o diagnóstico da situação de controles em um ambiente de negócios que é suportado por sistemas aplicativos.

Todas as empresas e respectivos colaboradores e interessados serão, com certeza, beneficiados.

6. Referências

AMARAL JUNIOR, Geraldo Lemos. **Sistema Gerencial de Controle**. São Paulo: Papel Virtual Editora, 2003.

BEAL, Adriana. **Segurança da Informação**. São Paulo: Atlas, 2005.

BHATIA, Mohan. **Auditing in a Computerised Environment**. New Delhi: Tata McGraw Hill, 2002.

CANNON, David. **CISA Certified Information Systems Auditor Study Guide**. Indianapolis – Indiana. Wiley Publishing Inc. 2011

CMMI – "Capability Maturity Models Integration", disponível em: (http://www2.lsd.ufcg.edu.br/~renato/CMMI.pdf)

COBIT – **Governance, Control and Audit for Information and Related Technology – IT**

CODERRE, David G. **CAATTs and Other BEASTs for Auditors**. Vancouver: Ekaros, 2005

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação.** Rio de Janeiro. Axcel Books. 2000.

FONTES, Edison. **Segurança da Informação.** São Paulo: Sicurezza, 2000.

Gestáo de "TIC": ITIL – **IT Infrastructure Library – OGC: Office of Government Commerce, UK. Vídeo em português.** Disponível em: http://www.youtube.com/watch?v=B0vF7xaloFU Acesso em: 9/05/2015.

Gestão de continuidade de negócios: **Código de prática. ABNT NBR 15999-1:2007**. Disponível em: http://www.abntcatalogo.com.br/norma.aspx?ID=533. Acesso em: 20/04/2015

Gestão de Governança – Controles internos. Disponível em: http://www.coso.org/. Acesso em: 20/04/2015

Gestão de riscos de segurança da informação. **ABNT NBR ISO/IEC 27005:2011**. Disponível em: http://www.27000.org/iso-27005.htm. Acesso em 20/04/2015

Gestão de Riscos. **ABNT NBR ISO/IEC 31000:2009**. Disponível em: http://www.iso.org/iso/home/standards/iso31000.htm. Acesso em: 20/04/2015

Gestão de Segurança da Informação. NBR ISO/IEC 27000. Disponível em: http://iso27000.com.br/ . Acesso em: 11/03/2015

Gestão de Sistemas de Qualidade - **Requisitos. ABNT NBR ISO 9001:2008** Disponível em: http://www.abntcatalogo.com.br/norma.aspx?ID=51639. Acesso em: 20/04/2015.

Governance Institute, ISACA, Version 5.0. Disponível em: http://www.isaca.org/cobit/pages/default.aspx. Acesso em: 11/03/2015

ISACA. **CISA Review Manual 2012**. Rolling Meadows – Illiois. ISACA. 2011

ISACA. **Padrões para Auditoria de Sistemas de Informação**, Disponível em http://www.isaca.org/Standards for IS Auditing (Portuguese).htm, Acesso em 24/04/2015.

LANZA, Richard B. **101 ACL Applications: A toolkit for today's Auditor**. Vancouver: Global Audit, 2000.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna,2008

MCNAMEE, David; PLEIER, Joseph R. **Risk Management: Best Practices, Case Studies and Related Materials**. Vancouver: Pleier Corporation, 1999.

NEVES, Roberto C. **Crises Empresariais com a Opinião Pública**. Rio de Janeiro: Mauad, 2002.

PECK, Patrícia. **Direito Digital**. São Paulo: Saraiva, 2002.

PELTIER, Thomas R. **Information Security Risk Analysis**. Michigan: CRC Press, 2001.

Portal GSTI – **Compartilhamento do conteúdo com foco em TI para profissionais e estudantes da área**. Disponível em: http://www.portalgsti.com.br/2013/12/ISO-27000.html. Acesso em: 11/03/2015

Procedimentos de Auditoria Informática – **Câmara Brasileira de Auditoria Informática-Instituto dos Auditores Internos do Brasil** – AUDIBRA.

SÊMOLA, Marcos. **Gestão da Segurança da Informação.** Rio de Janeiro: Editora Campus, 2004.

Sistema de Gestão Ambiental. **ABNT NBR ISO 14001**. Disponível em: http://www.abnt.org.br/m3.asp?cod_pagina=1006. Acesso em: 20/04/2015

SPAFFORD. G. **The Benefits of Standard IT Governance Frameworks**, Disponível em http://www.itpi.org/, Acesso 10/04/2015.

WOOD, Charles Cresson. **Information Security Policies Made Easy**. San Jose: Information Shield, 2002.

APÊNDICE A – Questionário Dirigido às Instituições

Tabela 5: Levantamento Primário

Questão	Não Sei	Não	Sim
Sua empresa tem auditoria interna?	0%	50%	50%
Se tiver auditoria interna, tem alguém especializado em Auditoria de TI e/ou Sistemas?	0%	38%	62%

Fonte: Elaborado pelo autor em conjunto com o orientador.

Tabela 6: Complementação das Respostas Positivas – 1

Itens revisados pela auditoria interna	Nº de Empresas
Controle de acesso aos sistemas	5
Não se aplica	3
Recertificação periódica dos acessos	4
Controle de usuários privilegiados	5
Controle de antivírus	4
Controle administrativo e/ou operacional de senhas	3

Fonte: Elaborado pelo autor em conjunto com o orientador.

Tabela 7: Complementação das Respostas Positivas – 2

Questão	Não Sei	Não	Sim
Sua empresa tem auditoria externa?	0%	25%	75%
Se tem auditoria externa, tem algum profissional que realiza alguma revisão relacionada a Auditoria de TI?	0%	37%	63%
Sua empresa tem processos suportados por sistemas aplicativos?	0%	0%	100%
Sua empresa tem política de segurança da informação?	0%	0%	100%
Se sim, é atualizada anualmente?	0%	63%	37%
Ainda dobre política de segurança da informação. Ela está disponível para todos os usuários e os profissionais de TI?	0%	12%	88%
Sua empresa tem alguma norma de conduta ética ou similar?	12%	0%	88%
Se sim, é atualizada anualmente?	12%	63%	25%
Ainda sobre norma de conduta e ética, ela está disponível para todos os usuários e profissionais de TI?	0%	25%	75%
Se existe algum processo, é revisado periodicamente a cada dois anos?	12%	0%	82%
Caso exista algum processo, o mapeamento identifica os pontos de controle necessários para a correta gestão do processo?	12%	0%	88%
Cada um dos sistemas aplicativos possui proprietário formalmente definido?	0%	0%	100%
Cada um dos sistemas aplicativos tem administrador de segurança formalmente definido?	12%	38%	50%

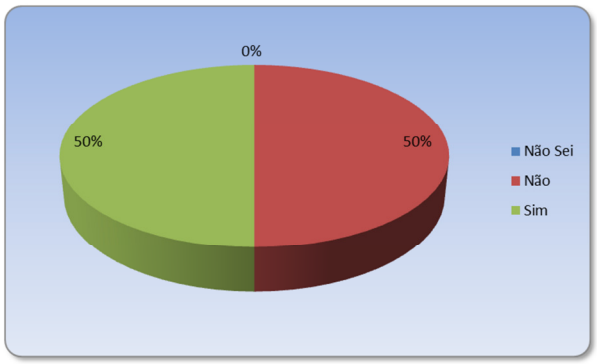
Fonte: Elaborado pelo autor em conjunto com o orientador

Tabela 8: Questões referentes aos sistemas informatizados

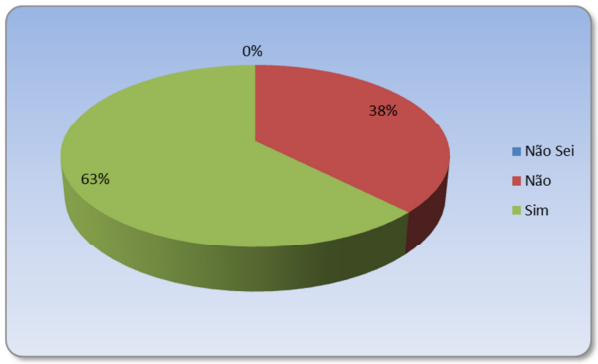
Questão	Não Sei	Não	Sim
Cada acesso concedido é formalmente solicitado pelo gestor do usuário solicitante?	0%	0%	100%
Cada acesso concedido é formalmente aprovado pelo proprietário do sistema aplicativo (ou pro alguém que o represente formalmente)	0%	0%	100%
Cada acesso concedido tem comprovação da autorização do proprietário?	12%	0%	88%
Os acessos vigentes são revisados a cada seis meses ou um ano?	0%	50%	50%
Existe processo de recertificação anual feito pelos proprietários ou pelo menos conduzido por alguém que coordene essa tarefa?	25%	63%	12%
É conduzida alguma auditoria ou revisão para verificar se todos os acessos vigentes estão suportados por autorização do proprietário?	37%	25%	38%

Fonte: Elaborado pelo autor em conjunto com o orientador

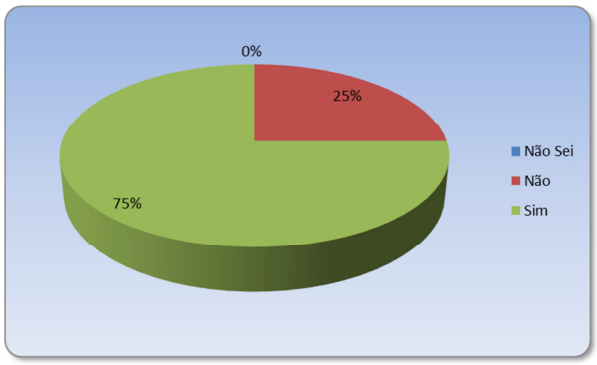
A fim de melhor visualização das respostas, essas serão apresentadas através dos gráficos a seguir:



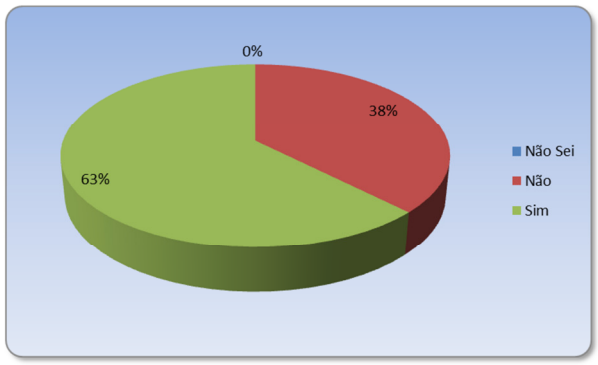
Questão 1: Sua empresa tem auditoria interna?
Fonte: Elaborado pelo autor em conjunto com o orientador



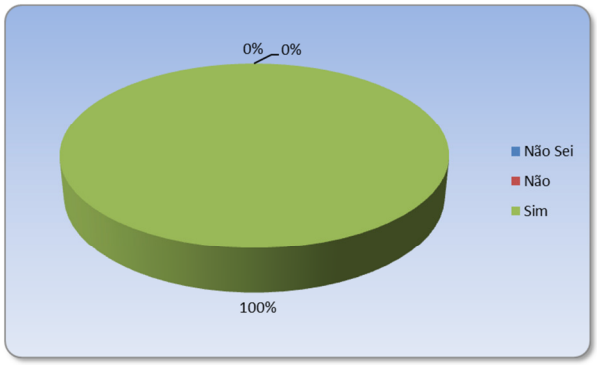
Questão 2: Se tem Auditoria Interna, tem alguém especializado para Auditoria de TI e/ou Sistemas?
Fonte: Elaborado pelo autor em conjunto com o orientador



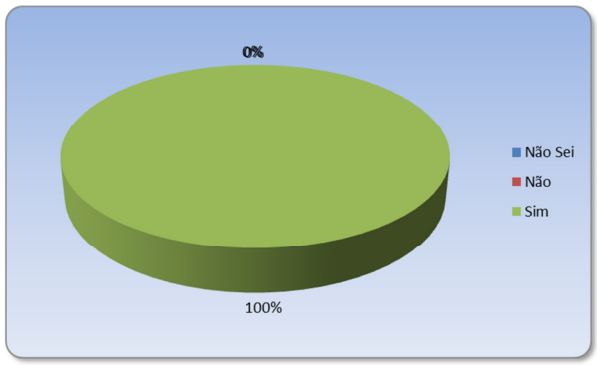
Questão 3: Sua empresa tem Auditoria Externa?
Fonte: Elaborado pelo autor em conjunto com o orientador



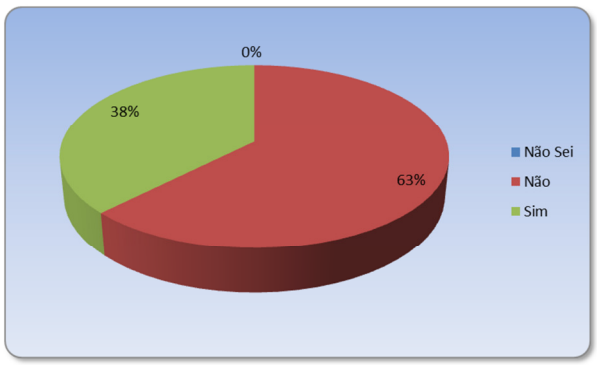
Questão 4: Se tem Auditoria Externa, tem algum profissional que realiza alguma revisão relacionada a Auditoria de TI?
Fonte: Elaborado pelo autor em conjunto com o orientador



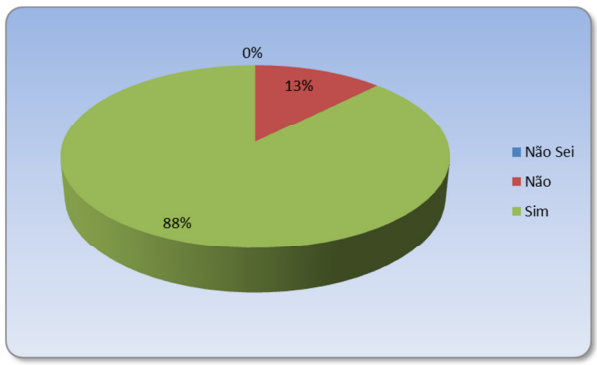
Questão 5: Sua empresa tem Processos suportados por Sistemas Aplicativos?
Fonte: Elaborado pelo autor em conjunto com o orientador



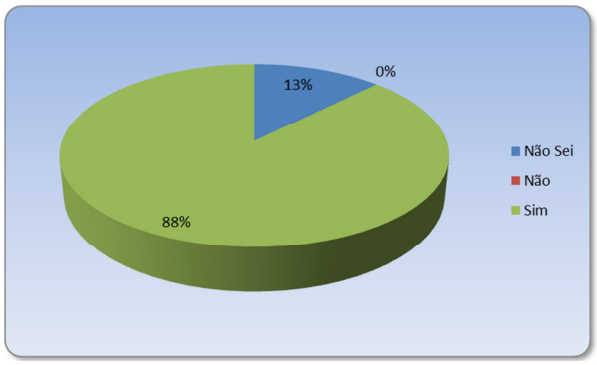
Questão 6: Sua empresa tem alguma Política de Segurança da Informação?
Fonte: Elaborado pelo autor em conjunto com o orientador



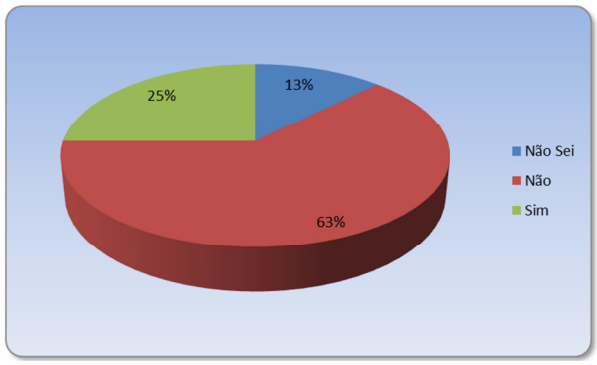
Questão 7: Se sim, é atualizada anualmente?
Fonte: Elaborado pelo autor em conjunto com o orientador



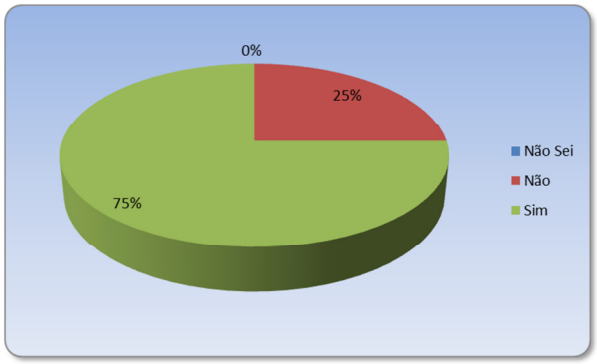
Questão 8: Ainda sobre Política de Segurança da Informação. Ela está disponível para todos os usuários e os profissionais de TI?
Fonte: Elaborado pelo autor em conjunto com o orientador



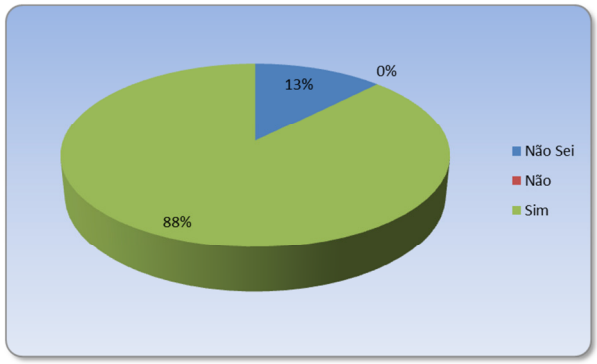
Questão 9: Sua empresa tem alguma Norma de Conduta Ética ou similar?
Fonte: Elaborado pelo autor em conjunto com o orientador



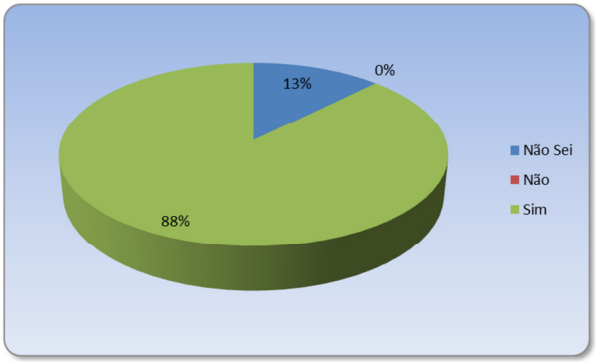
Questão 10: Se sim, é atualizada anualmente?
Fonte: Elaborado pelo autor em conjunto com o orientador



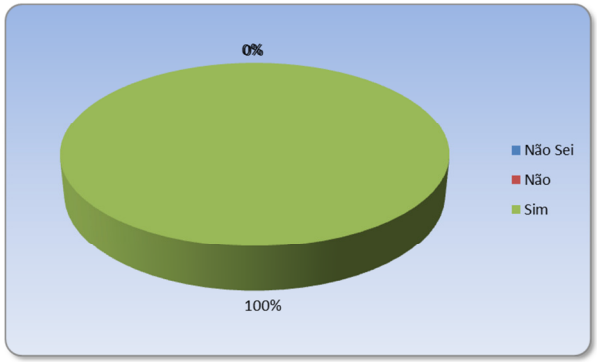
Questão 11: Ainda sobre a Norma de Conduta e Ética, ela está disponível para todos os usuários e os profissionais de TI?
Fonte: Elaborado pelo autor em conjunto com o orientador



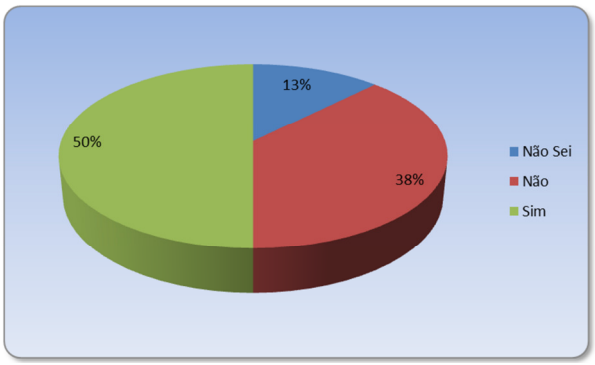
Questão 12: Se existe algum processo, é revisado periodicamente, pelo menos a cada 2 anos?
Fonte: Elaborado pelo autor em conjunto com o orientador



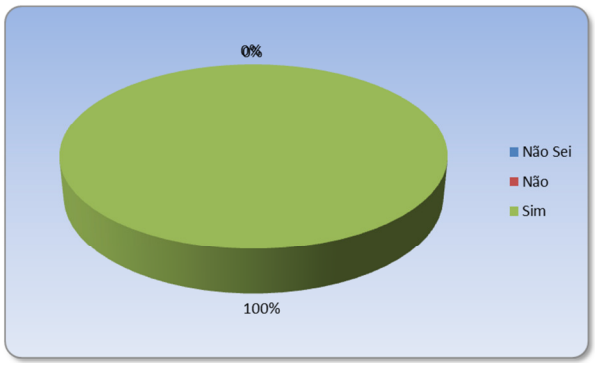
Questão 13: Se existe algum processo, o mapeamento identifica os pontos de controle necessários para a correta gestão do processo?
Fonte: Elaborado pelo autor em conjunto com o orientador



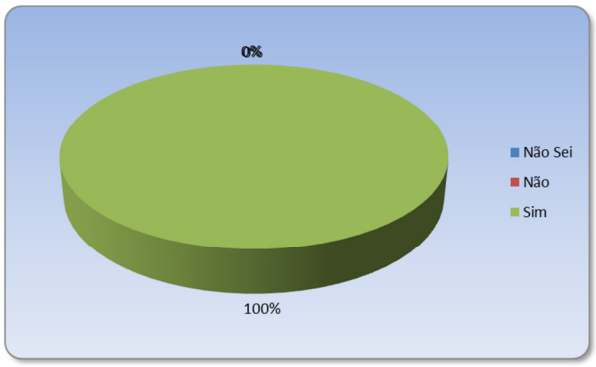
Questão 14: Cada um dos Sistemas Aplicativos tem proprietário formalmente definido?
Fonte: Elaborado pelo autor em conjunto com o orientador



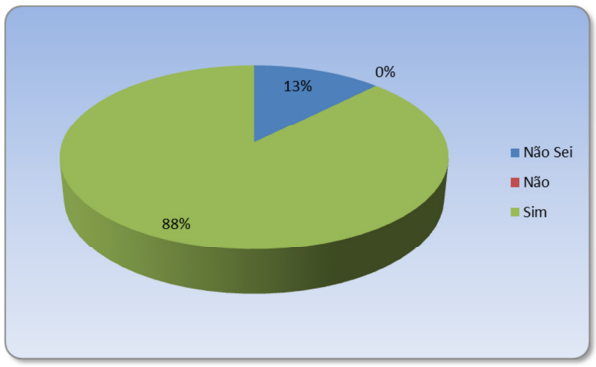
Questão 15: Cada um dos Sistemas Aplicativos tem administrador de segurança formalmente definido?
Fonte: Elaborado pelo autor em conjunto com o orientador



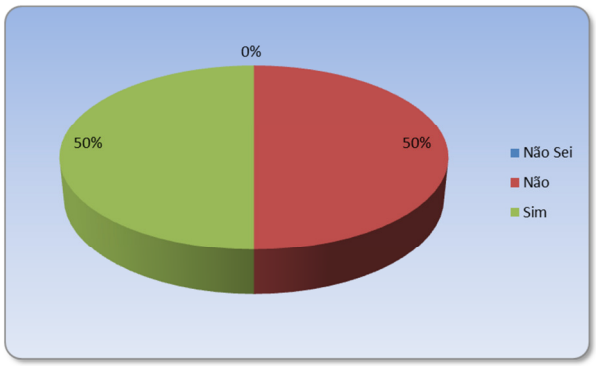
Questão 16: Cada acesso concedido é formalmente solicitado pelo Gestor do usuário requisitante?
Fonte: Elaborado pelo autor em conjunto com o orientador



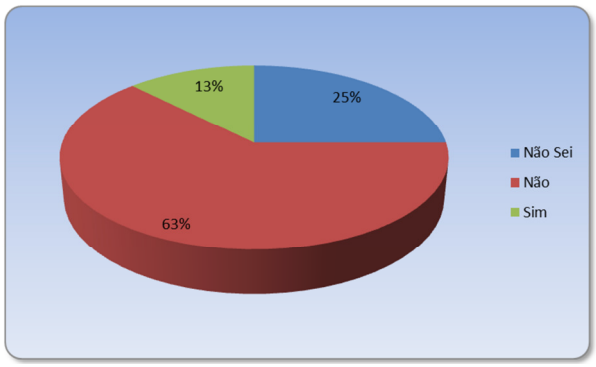
Questão 17: Cada acesso concedido é formalmente aprovado pelo Proprietário do Sistema Aplicativo (ou por alguém que o represente formalmente?)
Fonte: Elaborado pelo autor em conjunto com o orientador



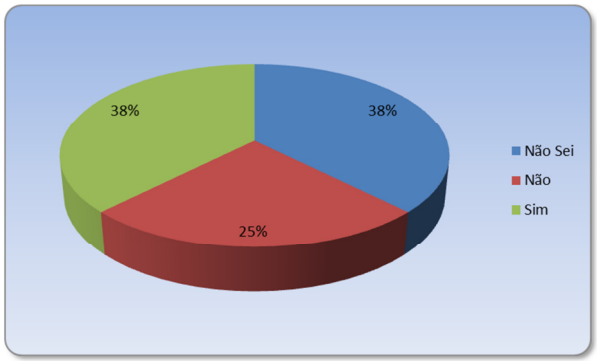
Questão 18: Cada acesso concedido tem comprovação da autorização do Proprietário?
Fonte: Elaborado pelo autor em conjunto com o orientador



Questão 19: Os acessos vigentes são revisados a cada 6 meses (ou um ano)?
Fonte: Elaborado pelo autor em conjunto com o orientador



Questão 20: Existe processo de re-certificação anual, feito pelos Proprietários (ou, pelo menos, conduzido por alguém que coordene esta tarefa)?
Fonte: Elaborado pelo autor em conjunto com o orientador



Questão 21: É conduzida alguma auditoria ou revisão para verificar se todos os acessos vigentes estão suportados por uma autorização do Proprietário?
Fonte: Elaborado pelo autor em conjunto com o orientador

LISTA DE QUADROS

O grau de abrangência e profundidade dos questionários básicos (são mostrados alguns exemplos) depende da cultura atual da organização em relação aos Sistemas de Informação em termos de controles e eficiência, ao conhecimento das Políticas e Normas da empresa, ao estágio de modernidade da tecnologia (*hardware*, *software*, rede, etc.) e ao estado de conscientização e comprometimento dos gestores e usuários dos sistemas de "TIC".

A ideia é iniciar com questionários simples, claros e de fácil compreensão, submetidos aos gestores de Sistemas Aplicativos de Negócios, suportados pela presença e auxílio dos profissionais da área de "TIC" que suportam tecnicamente estes sistemas. A partir daí, ao longo do tempo, com a melhora do conhecimento, os questionários podem ser mais detalhados e aprofundados.

É fundamental estabelecer um critério para definir o "grau de maturidade" atual (no momento da resposta) para cada item do questionário. Para uma melhor avaliação do diagnóstico, as respostas não podem se limitar a um "sim" ou "não", sendo assim podem ser incluídas gradações como, por exemplo:

"0" – não tem/não possui documentação à respeito; as pessoas fazem o serviço conforme aprenderam de outras pessoas;

"1" - existe alguma coisa documentada, embora de modo informal, sem aprovação adequada e documentação incompleta;

"2" existem políticas e/ou procedimentos embora sem controles e monitoramentos eficazes para garantir a conformidade;

"3" existem controles que auxiliam o monitoramento em relação à aderência às Políticas e Normas, entretanto, não são garantidas as análises sobre os resultados.

Essa gradação pode ser estendida até um nível máximo "n" que atesta a completude da atividade, devidamente aprovada, documentada, revisada periodicamente e com controles que asseguram sua eficácia e monitoramento efetivo.

Também pode ser considerada a resposta "N/A" ("não se aplica"), dependendo da pergunta. Igualmente, podem ser acrescentadas colunas, como por exemplo, uma

coluna de “grau de maturidade” esperado para uma próxima avaliação, o que representaria o índice de progresso esperado no próximo diagnóstico.

Normalmente as empresas julgam que um progresso de mais de um nível (considerando o exemplo dado, passando do nível “1” para “3”) é muito rápido e fácil. Por este motivo, é importante a presença dos profissionais (tanto da área de negócio como do e “TIC”) para avaliar melhor os custos, prazos e benefícios de planos de ação decorrentes das avaliações e o progresso pretendido.

Um exemplo para a primeira planilha abaixo: Caso a empresa possua uma Política de Segurança da Informação aprovada nos níveis competentes, mas sem publicação adequada, o progresso para atingir um grau de maturidade de mais de um nível não demanda altos custos e prazos caso a organização opte por publicá-la na Intranet da empresa para que todos os envolvidos tenham acesso assim que precisarem. Caso a empresa não tenha Intranet, os custos e prazos serão maiores e a progressão do aperfeiçoamento será mais complexa, pois depende da implantação da Intranet corporativa. Também devem ser considerados os casos de pessoas que não possuem acesso à rede da “TIC” (operários de chão de fábrica, estagiários administrativos, etc.).

Quadro 1: Política de Segurança da Informação

Avaliação: Segurança TI			**Responsável**	
Área: Política de Segurança da Informação			**Respondente**	
Observações sobre a área:				
ID	**Questionamentos básicos**	**Grau deMaturidade**	**Comentários**	**Referência dos Papeis de Trabalho**
POLIT-01	**DOCUMENTAÇÃO DA POLÍTICA:**			
	Está aprovada nos níveis competentes?			
	Está publicada adequadamente?			
	Tem o comprometimento formal da Alta Direção?			

Fonte: Elaborado pelo autor em conjunto com o orientador.

Quadro 2: Controle de Acesso à Informação

Avaliação: Segurança TI			**Responsável**	
Área: Controle de Acesso à Informação			**Respondente**	
Observações sobre a área:				
ID	**Questionamentos básicos**	**Grau deMaturidade**	**Comentários**	**Referência dos Papeis de Trabalho**
ACESS-01	**PROCEDIMENTOS GERAIS PARA QUALIFICAR O ACESSO**			
	Há definição documentada dos requisitos do negócio para concessão e controle de acesso?			
	Os procedimentos consideram os requisitos de segurança de aplicações específicas do negócio?			
	Garantem as obrigações contratuais e a legislação vigente em relação à proteção do acesso a dados ou serviços?			

Fonte: Elaborado pelo autor em conjunto com o orientador.

Quadro 3: Controle de Acesso aos Sistemas Aplicativos de Negócio - SAN

Avaliação: Segurança TI			Responsável	
Área: Controle de Acesso aos Sistemas Aplicativos de Negócio - SAN			Respondente	
Observações sobre a área:				
ID	Questionamentos básicos	Grau deMaturidade	Comentários	Referência dos Papeis de Trabalho
ACE-SAN-01	QUALIFICAÇÃO DE ACESSO AO APLICATIVO - "SAN"			
	Há garantia de que o acesso lógico a SW e informações seja restrito aos usuários autorizados?			
	Há garantia de que os "SAN"s bloqueiem acesso não autorizado e registrem as tentativas realizadas?			
	Os "SAN"s permitam acessos somente às entidades "indivíduo-usuário" nominalmente autorizados?			

Fonte: Elaborado pelo autor em conjunto com o orientador.

Quadro 5: Classificação e Controle dos Ativos de Informação

Avaliação: Segurança TI			Responsável	
Área: Classificação e Controle dos Ativos de Informação			Respondente	
Observações sobre a área:				
ID	Questionamentos básicos	Grau deMaturidade	Comentários	Referência dos Papeis de Trabalho
CLASS-01	INVENTÁRIO DOS TIPOS DE INFORMAÇÕES			
	Está atualizado, disponível e identifica os respectivos proprietários responsáveis?			
	Cada ativo tem sua classificação devidamente acordada e documentada?			
	Está disponível para todos?			

Fonte: Elaborado pelo autor em conjunto com o orientador.

Quadro 4: Acordos de Níveis de Serviço

Avaliação: Segurança TI			Responsável	
Área: Acordos de Níveis de Serviço - SLA "Service Level Agreement"			Respondente	
Observações sobre a área:				
ID	Questionamentos básicos	Grau deMaturidade	Comentários	Referência dos Papeis de Trabalho
ANV-01	EXISTÊNCIA DE SLA			
	Há processo de gerenciamento dos Acordos de Níveis de Serviço ("SLA's")?			
	O processo é formalizado e de conhecimento dos interessados e envolvidos?			
	Estão assinados e revisados anualmente?			

Fonte: Elaborado pelo autor em conjunto com o orientador.