UNISA - UNIVERSIDADE DE SANTO AMARO

SISTEMAS DE INFORMAÇÃO

GRASIELI CRISTINI LUIZ

RAFAEL SALVINO

UM ESTUDO SOBRE A MITIGAÇÃO DE RISCOS INERENTES À SEGURANÇA DA INFORMAÇÃO EM UMA EMPRESA DE PEQUENO PORTE NA ÁREA DE PRESTAÇÃO DE SERVIÇO DE ACESSO À INTERNET

São Paulo

2012

GRASIELI CRISTINI LUIZ

RAFAEL SALVINO

UM ESTUDO SOBRE A MITIGAÇÃO DE RISCOS INERENTES À SEGURANÇA DA INFORMAÇÃO EM UMA EMPRESA DE PEQUENO PORTE NA ÁREA DE PRESTAÇÃO DE SERVIÇO DE ACESSO À INTERNET

Trabalho de Conclusão de Curso apresentado para obtenção do título de Bacharel em Sistemas de Informação da Universidade de Santo Amaro, sob a orientação do Prof. Marlom Alves Konrath.

São Paulo

2012

GRASIELI CRISTINI LUIZ

RAFAEL SALVINO

UM ESTUDO SOBRE A MITIGAÇÃO DE RISCOS INERENTES À SEGURANÇA DA INFORMAÇÃO EM UMA EMPRESA DE PEQUENO PORTE NA ÁREA DE PRESTAÇÃO DE SERVIÇO DE ACESSO À INTERNET

Trabalho de Conclusão de Curso apresentado para obtenção do título de Bacharel em Sistemas de Informação da Universidade de Santo Amaro – UNISA.

Data de Aprovação:

BANCA EXAMINADORA

_____

Professor
Marlom Alves Konrath

_____

Professora
Denise Canal

_____

Professora
Itsche Baran

CONCEITO FINAL: _____

Eu Grasieli, dedico este trabalho a minha filha Julia, que esteve no meu ventre durante 9 meses do curso, nasceu e continua me acompanhando em todos os instantes. Obrigada por ter proporcionado que eu vivenciasse os momentos mais felizes da minha vida. Por ter me dado forças para seguir em frente quando pensei em desistir.

Eu Rafael, dedico este trabalho aos meus pais que foram verdadeiros pilares para minha formação acadêmica e humana.

Agradeço por terem sido os maiores promotores de meu desenvolvimento e minha base em qualquer momento.

AGRADECIMENTOS DA GRASIELI

Agradeço a Deus pelo dom da vida, por seu infinito amor e por ter permitido que eu chegasse até aqui.

Agradeço aos meus pais Mauro e Dora por serem exemplos de vida, pela doação de suas vidas, investindo em mim, quase sempre, mais do que podiam. Por suas orações e por todo amor e carinho que me dedicam.

Agradeço aos meus irmãos Gleicilaine, Kleiton e Gabriela porque mesmo com todos os contratempos sempre estão ao meu lado.

Ao meu sobrinho Murilo e minha filha que me alegram todos os dias.

Agradeço especialmente ao Professor Marlom Konrath, meu orientador por sua enorme paciência, por sua disponibilidade e por transmitir seus conhecimentos durante a realização desse trabalho.

Obrigado a todos que mesmo não estando citados aqui contribuíram para a conclusão de mais uma etapa da minha vida.

AGRADECIMENTOS DO RAFAEL

Agradeço a Nosso Senhor por todos os auxílios que Sua divina providência me concedeu durante e para esse trabalho, pela maternal intercessão de Maria Santíssima.

Agradeço aos meus pais que me proporcionaram os meios necessários para a conclusão desse trabalho, desde a estrutura familiar à financeira.

Agradeço de modo especial ao professor Marlom Konrath, que orientou na condução desse trabalho. Como sabiamente dizia o *doctor Angelicus* "A humildade é o primeiro degrau para a sabedoria", esse trabalho só pode ser possível graças uma posição de humildade diante da sábia orientação dele.

Por fim agradeço a todos não citados anteriormente, que de forma direta ou indireta contribuíram para que chegasse a conclusão dessa fase em minha vida.

Ninguém ignora tudo. Ninguém sabe tudo. Todos nós sabemos alguma coisa. Todos nós ignoramos alguma coisa. Por isso aprendemos sempre.

PAULO FREIRE

RESUMO

Palavras-chave:

Cada vez mais as empresas usam TI como suporte aos seus negócios. No entanto, grande parte delas desconhece os riscos ao qual está exposta no que tange a segurança de seus ativos. Este desnivelamento entre a necessidade e a prática das organizações perante a gestão de risco tem deixado muitas empresas vulneráveis, pois se ela não se preocupa de saber onde estão suas dificuldades e falhas operacionais poderá sofrer mais com perdas que, no mínimo, a tornarão menos competitiva.

Neste trabalho foi desenvolvido um estudo de caso sobre a análise de risco em uma empresa de pequeno porte no setor de Tecnologia da Informação, com o intuito de identificar os maiores riscos aos quais está exposta. A análise foi realizada visando a proteção dos ativos e a continuidade da operação dos principais serviços da organização, com observância direta as normas técnicas e as melhores práticas sugeridas pela metodologia adotada.

Através do estudo da metodologia adotada e da análise realizada foi desenvolvida uma base para definição dos níveis de criticidade e impacto existentes. *A posteriori* as informações coletadas serviram de fonte para criação de medidas estratégias na diminuição de impacto dos riscos. Os resultados se mostraram adequados ao propósito deste trabalho.

ABSTRACT

Keywords:

Companies are increasing its dependency in IT as a support for their business. However, most of them are not aware of the risks they are exposed in regards to the security of their assets. This unevenness between the need and the practice of risk management has left many companies vulnerable, because if they do not know where are their operational failures, will they suffer losses that, at minimum, will make them less competitive.

This work developed a case study about the risk analysis of a small company on the field of Information Technology, in order to mitigate the major risks that it is susceptible. The analysis was performed aiming to protect the assets and the continued operation of the organization's main services, with direct compliance to the technical standards and best practices suggested by the selected methodology.

Based on the studied methodology and on the performed analysis a base for the definition of the criticality levels and their impact was developed. *A posterior* the collected information served as source for the creation of strategic measures to reduce the impact of the risks. The results were considered appropriate to the purpose of this work.

LISTA DE ILUSTRAÇÕES

FIGURA 1 - COSO - ENTERPRISE RISK MANAGEMENT FRAMEWORK 28
FIGURA 2 - O MODELO DE AVALIAÇÃO DE RISCO COBRA 33
FIGURA 3 - PRINCÍPIOS E ATRIBUTOS DA AVALIAÇÃO DE RISCO DA SEGURANÇA DA INFORMAÇÃO 38
FIGURA 4 - FASES OCTAVE 40
FIGURA 5 - TOPOLOGIA LÓGICA DA INFRAESTRUTURA DA IOL 44

LISTA DE TABELAS

TABELA 1 - EXEMPLOS DE EVENTOS CORRIQUEIROS 18
TABELA 2 - TABELA MULTIPLICADORA DE PERDA ANUAL 25
TABELA 3 - RISCO 1 51
TABELA 4 - RISCO 2 52
TABELA 5 - RISCO 3 52
TABELA 6 - RISCO 4 52
TABELA 7 - RISCO 5 53
TABELA 9 - RISCO 6 53
TABELA 10 - RISCO 7 53
TABELA 11 – AVALIAÇÃO DE RISCO 1 54
TABELA 12 - AVALIAÇÃO DE RISCO 2 54
TABELA 13 - AVALIAÇÃO DE RISCO 3 54
TABELA 14 - AVALIAÇÃO DE RISCO 4 54
TABELA 15 - AVALIAÇÃO DE RISCO 5 54
TABELA 16 - AVALIAÇÃO DE RISCO 6 55
TABELA 17 - AVALIAÇÃO DE RISCO 7 55

LISTA DE SIGLAS E ABREVIATURAS

ABNT - Associação Brasileira de Normas Técnicas

ASN - *Autonomous System Number*

COBRA - Consultative, Objective and Bi-functional Risk Analysis.

COSO - *Comittee of Sponsoring Organizations of the Treadway Commission*

DSIC - Departamento de Segurança da Informação e Comunicações

EPA - Exposição de Perda Anual.

EPU - Expectativa de Perda Única

FE - Fator de Exposição

FRAP - *Facilitated Risk Assessment Process*

GCN - Gerenciamento de Continuidade de Negócios

GSIPR - Gabinete de Segurança Institucional da Presidência da República

IEC - *International Electrotechnical Commission*

IOL - Itapecerica Online Telecomunicação e Informática LTDA

ISO - Organização Internacional para Padronização

OCTAVE - *Operationally Critical Threat, Asset, and Vulnerability Evaluation*

OSPF – *Open Shortest Path First*

PABX - *Private Automatic Branch eXchange*

PCN - Plano de Continuidade de Negócios

TOA - Taxa de Ocorrência Anual

VA - Valor do Ativo

SUMÁRIO

1 INTRODUÇÃO 14
1.1 ESTRUTURA DO TCC 16
2 REVISÃO BIBLIOGRÁFICA 17
2.1 GESTÃO DA CONTINUIDADE DE NEGÓCIOS 17
2.1.1 Definição 17
2.1.2 Sistemas de GCN 19
2.2 RISCOS 21
2.2.1 Gestão de riscos. 22
2.3 METODOLOGIAS DE AVALIAÇÃO DE RISCO 26
2.3.1 OCTAVE 26
2.3.2 COSO 28
2.3.3 FRAP 29
2.3.4 COBRA 31
2.4 SOLUÇÃO ESCOLHIDA: 33
2.5 A SITUAÇÃO DA IOL PERANTE A MATURIDADE E RECURSOS: 34
2.5.1 COSO 34
2.5.2 FRAP 34
2.5.3 COBRA 35
2.5.4 OCTAVE 35
3 A EMPRESA 43
3.1 TOPOLOGIA 43
3.2 ESCOLHA E JUSTIFICATIVA 44
3.3 PERSPECTIVAS 44
4 CONTROLES PARA A MITIGAÇÃO DOS RISCOS 46
4.1 GESTÃO DE CONHECIMENTO: 46
4.1.1 Política de Segurança da Informação 46
4.1.2 Treinamento de Pessoal 47
4.1.3 Compartilhamento de Conhecimento 47
4.2 GESTÃO DE PESSOAS 47
4.2.1 Papéis e Responsabilidades 47

4.2.2 Assegurar a conformidade de responsabilidade 47
4.3 GESTÃO DE DESEMPENHO 48
4.3.1 Monitoramento do uso do sistema 48
4.3.2 Identificar e implementar melhorias de desempenho 48
4.4 GESTÃO DE RELACIONAMENTO 48
4.4.1 Seleção de Provedor de Serviços 48
4.4.2 Revogação dos direitos 48
4.5 GESTÃO DE TECNOLOGIA 49
4.5.1 Manutenção de disponibilidade do ativo 49
4.5.2 Continuidade dos Serviços 49
4.5.3 Entrega do Serviço 49
4.6 GESTÃO DE AMEAÇAS 49
4.6.1 Política de Controle de Acesso 49
4.6.2 Riscos causados por colaboradores 49
4.7 PRÁTICAS DE CONTRATO 50
4.7.1 Estabelecimento de contrato 50
4.7.2 Acordo de níveis de serviços 50
4.7.3 Acordo de confidencialidade 50
4.7.4 Condições de contratação 50
5 ESTUDO DE CASO 51
5.1 IDENTIFICAÇÃO DOS RISCOS 51
5.2 AVALIAÇÃO DOS RISCOS 54
5.3 TRATAMENTO DOS RISCOS 55
6 CONSIDERAÇÕES FINAIS 59
6.1 TRABALHOS FUTUROS: 60
REFERÊNCIAS 61
ANEXOS 64

1 INTRODUÇÃO

A área de Tecnologia da Informação, nos últimos anos, tem impactado profundamente o modo como as empresas se estruturam e fazem negócios. O uso do computador e mais recentemente da Internet está disseminado em praticamente todos os setores das organizações. Nos dias atuais, TI é cada vez mais responsável por fornecer suporte ao negócio em nível mundial, ou seja, sem esse serviço as organizações ficariam inoperantes ou com baixo grau de produtividade.

Mesmo estudos no mercado brasileiro apontam a forte presença da TI como componente estratégico para as empresas, especialmente na última década:

> As organizações têm buscado um uso cada vez mais intenso e amplo da Tecnologia de Informação, utilizando-a como uma poderosa ferramenta que altera as bases de competitividade, estratégicas e operacionais das empresas (ALBERTIN, 2001, p. 43).

Torna-se cada vez mais perceptível que TI não é um ponto periférico dentro das empresas, mas uma pilastra fundamental para o funcionamento ordinário e extraordinário das atividades, por isso é importante que ela funcione de forma eficiente e com disponibilidade contínua.

No entanto, a maioria das empresas não possui planos para tratar situações em que o ambiente atual de TI seja severamente afetado e, ainda pior, desconhecem até mesmo os riscos a que estão expostas. Para sanar esta deficiência, a empresa deve passar por um processo formal de análise de segurança e elaborar um plano para gerenciá-lo, caso ocorra.

Tal análise e seu resultado, conhecido como Plano de Continuidade de Negócios, são de primordial importância, pois buscam garantir o funcionamento da organização em cenários críticos de forma que, na ocorrência de algum tipo de problema, a empresa continue funcionando com o mínimo de impacto possível.

Embora esse levantamento seja de basilar importância para a continuidade das operações da organização, segundo OS&T Informática (OS&T 2011), uma consultoria especializada em soluções de Segurança, em 2011, somente 30% do mercado brasileiro possuía um PCN e 57% encontrava-se em planejamento em meio às dificuldades, aos crescentes ataques, de ordem interna e externa. Já

segundo o Ponemon Institute (PONEMON, 2011) ataques atingem cerca de 90% das organizações, causado essencialmente pela ausência do conhecimento da própria empresa. Segundo a mesma pesquisa, atualmente cerca de 59% das empresas sofreram mais de duas violações entre julho de 2010 a julho de 2011.

Diante dessa questão, é evidente que é necessário para as organizações conhecer onde existem potenciais riscos para evita-los ou reduzir parte de seu impacto caso ocorram. Tendo em vista esse cenário, torna-se mais clara a ideia do quanto é importante a realização de uma análise de riscos.

O presente trabalho apresenta um estudo de caso, realizado na empresa IOL (Itapecerica Online Telecomunicação e Informática LTDA), que não possui os riscos do negócio mapeados. O estudo de caso contemplou a análise dos principais riscos do negócio da empresa em questão, utilizando-se para isso a metodologia OCTAVE, detalhada no Capítulo 2.

A IOL é uma empresa de telecomunicações, que opera há 14 anos no mercado e que demonstrou perceptível interesse em realizar esse estudo. A análise foi conduzida com o apoio do atual administrador, através de entrevistas estruturadas e da composição de um grupo multidisciplinar, conforme recomenda a metodologia.

A principal contribuição deste trabalho é o mapeamento realizado na IOL, buscando elencar os principais riscos aos quais ela está suscetível. Este é um trabalho inédito na empresa em questão, já que até a sua realização ela não conhecia nem gerenciava estes riscos. Os resultados poderão servir de suporte para futuras tomadas de decisões, que busquem diminuir os riscos de negócio da IOL. Tanto na empresa, quanto no mercado brasileiro, atualmente este tipo de trabalho é pouco conhecido e explorado.

Além disso, para os autores, este trabalho permitiu a expansão do conhecimento na área de gerenciamento de riscos, sua relevância e como aplicá-lo numa empresa. Ao mesmo tempo em que trouxe uma bagagem intelectual, os autores creem que o mesmo será de grande valia em suas vidas profissionais, afinal a aptidão de uma empresa em sobreviver a desastres, bem como a rapidez que ela possui para restabelecer a funcionalidade de suas atividades tidas como críticas são o principal aspecto que diferencia se a esta irá conseguir manter suas atividades ou

sucumbir à falência e consequente interrupção de suas operações. Neste sentido a continuidade de negócios deve ser tratada como prioridade pelas empresas.

1.1 ESTRUTURA DO TCC

Este trabalho está estruturado da seguinte forma. O capítulo 2 apresenta os principais conceitos relacionados ao trabalho, definindo e demonstrando o que é um Plano de Continuidade de Negócios e normas relacionadas ao assunto. Introduz ainda definições sobre riscos, as principais metodologias estudadas para demonstrar qual a opção que mais se enquadra no assunto de análise de riscos, sendo assim, feita uma escolha da melhor solução para desenvolver de uma forma mais completa o método. No capítulo 3, é apresentado o estudo de caso da empresa escolhida, dando uma introdução de como funciona a empresa, desde sua área de atuação até um conhecimento mais profundo para aplicação da análise. O capítulo 4 apresenta os controles estudados e o capítulo 5 demonstra os riscos elencados e sugestões de mitigação para estes. Ao final, o Capítulo 6 apresenta o referencial bibliográfico utilizado e este trabalho termina com os anexos demonstrando os questionários utilizados na entrevista estruturada.

2 REVISÃO BIBLIOGRÁFICA

O capítulo 2 demonstra os conceitos básicos dos principais assuntos abordados nesta monografia. Para isso, primeiramente a Gestão da Continuidade de Negócios é abordada na Seção 2.1. A seguir, a seção 2.2 apresenta os conceitos e características dos Riscos, seguindo (Seção 2.3) para as Metodologias de Avaliação de Risco. A solução escolhida é apresentada na Seção 2.4 e este capítulo termina com a Seção 2.5 falando sobre a IOL, a empresa escolhida para o estudo de caso.

2.1 GESTÃO DA CONTINUIDADE DE NEGÓCIOS

É dever das organizações, possuírem planejamentos e mecanismos para adequarem-se à pronta recuperação das suas operações, no menor tempo possível, para se precaverem a eventos inesperados. Esse planejamento é feito através do Gerenciamento de Continuidade de Negócios (GCN).

2.1.1 Definição

Blyth (2009) definiu o Gerenciamento de Continuidade de Negócios como um sistema que declara a estrutura organizacional, bem como as respectivas responsabilidades de cada recurso humano, para permitir através dele a reação diante de situações de emergência tendo a possibilidade de conexão entre mitigação de risco, gestão da resiliência do negócio e retomada dos negócios.

O autor ressalta ainda que a GCN não deve ser encarada como um processo único, mas como um processo contínuo dentro da empresa, que deve ser guiado por um programa sobre as mudanças. Bon (2006) identificou os seguintes pontos como competência diretas do Gerenciamento de Continuidade de TI:

- Avaliar o risco e o impacto da ruptura dos serviços de Tl depois de um desastre.
- Identificar os serviços que são cruciais para o negócio e exigem medidas de prevenção adicionais.
- Definir períodos dentro dos quais os serviços precisam ser restaurados.

- Tomar medidas para prevenir, detectar, preparar-se para e mitigar os efeitos de desastres ou reduzir o seu impacto.
- Definir a abordagem a ser usada para restaurar os serviços.
- Desenvolver, testar e manter um plano de recuperação suficientemente detalhado para sobreviver a um desastre e restaurar os serviços normais depois de um período definido.

Matthys (2009) fez uma lista de tipos de incidentes mais corriqueiros e seus respectivos riscos:

Tabela 1 - Exemplos de eventos corriqueiros

Exemplos de eventos corriqueiros	
Evento	Risco
Equipamento quebrar, computador com problemas ou utilitário quebrado.	Nenhum dano e pouco impacto.
Computador com vírus e outras intrusões, fraude de dados. Governança corporativa inadequada.	Evento perturbador com maior impacto.
Falha na entrega de energia, gás, água, telefone e internet.	Dano de pendência no tipo de organização.
Inundação, incêndio, raio, e poluição do ar.	Plano de desastres, regulamentações e leis precisam ser respeitadas.
Atividades terroristas ou pandemias humanas ou em animais	Uma perturbação generalizada da comunidade
Evento perturbador que bloqueie a entrega de produto e serviços chaves.	Evento critico com um importante rico para sua organização.

Fonte: Adaptado de Matthys (2009).

Devido a clareza cada vez mais perceptível da necessidade do Gerenciamento da Continuidade de Negócios, em 2006 foi publicada a primeira norma de regulamentações do GCN, a GCN B5 25999, que tem como intuito manter a operabilidade do negócio nos momentos críticos.

2.1.2 Sistemas de GCN

Todo tipo de negócio está propício a sofrer diferentes tipos de interrupções, desde os mais catastróficos como incêndio e enchentes, até os de infraestrutura como problemas nos computadores, vírus, falha humana, etc. Sabendo disso, é possível imaginar que a empresa também sofrerá prejuízos financeiros.

Segundo STROHL Brasil (2011), a Gestão de Continuidade de Negócios (GCN) tem o propósito de manter as atividades da empresa dentro do seu funcionamento normativo caso ocorram essas interrupções, assim prevenindo de maiores prejuízos e criando um processo de GCN de acordo com cada perfil e necessidade do negócio. As seções a seguir apresentam as principais normas atuais de Gestão de Continuidade de Negócios.

2.1.2.1 NBR/ISO 15999-1 e NBR/ISO 15999-2

O Departamento de Segurança da Informação e Comunicações (DSIC), em parceria com o Gabinete de Segurança Institucional da Presidência da República (GSIPR), e a Associação Brasileira de Normas Técnicas (ABNT) criaram a norma NBR ISO/15999-1 (2007) no ano de 2007, com o objetivo de orientar as empresas fazendo uso de melhores práticas, caso haja algum tipo de incidente na organização, para que assim proporcione um melhor entendimento, para colaborar no desenvolvimento e implementação do GCN no negócio.

Já a norma NBR/ISO 15999-2 (2009) tem como finalidade garantir o funcionamento das operações do negócio mesmo com o surgimento de imprevistos graves na organização. Ou seja, ela permite que os principais processos da empresa continuem funcionando de forma normalizada, assim proporcionando a diminuição dos maiores prejuízos.

2.1.2.2 NBR/ISO 31000:2009

A ISO 31000:2009 (2009) entende que uma gestão de riscos eficaz tem que contemplar 11 princípios.

1. Uma gestão de riscos deve criar e proteger valor.
    - A preocupação com a realização demonstrável dos bens e sua melhoria de desempenho, por exemplo, a saúde e segurança de seus funcionários, a aceitação pública e a proteção do ambiente.
2. A gestão de riscos é parte integrante de todos os processos organizacionais.
    - A gestão de riscos deve ser encarada como responsabilidade da administração e parte integrante de todos os processos, principalmente o planejamento estratégico.
3. A gestão de riscos é parte da tomada de decisões.
    - Ela deve ser contemplada pelos tomadores de decisão em suas escolhas.
4. A gestão de riscos aborda explicitamente a incerteza.
    - Ela tem como obrigação avaliar as incertezas e a natureza de cada incerteza, para poder trata-la.
5. A gestão de riscos é sistemática, estruturada e oportuna.
    - A abordagem sistemática, oportuna e estruturada deve ser auxilio na contribuição rumo a eficiência e resultados mais consistentes.
6. A gestão de riscos baseia-se nas melhores informações disponíveis.
    - Os dados imputados no processo de gerenciamento de risco são baseados em fontes tidas como confiáveis de informação, tais como dados históricos, a experiência, as reações dos interessados, observação, previsões e opiniões de especialistas, contudo, é oportuno e necessário que os tomadores de decisão levantem as limitações dos dados utilizados e a divergência entre os especialistas, contudo, é oportuno e necessário que os tomadores de decisão levantem as limitações dos dados utilizados e a divergência entre os especialistas.
7. A gestão de riscos é feita sob medida.
    - Ela deve estar alinhada a filosofia operacional da empresa.
8. A gestão de riscos considera fatores humanos e culturais.
    - A gestão de riscos enxerga e reconhece as capacidades, percepções e intenções dos recursos humanos, tanto internos quanto externos.
9. A gestão de riscos é transparente e inclusiva.

- Os colaboradores devem saber o que ocorre em todas as fases da gestão de riscos, dando a possibilidade de eles expressarem-se.

10. A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças.
    - A gestão de riscos deve perceber e reagir diante das mudanças, na medida em que os eventos externos e internos ocorrem. Porque com o passar do tempo é natural que novos riscos surjam, alguns se modificam e outros desaparecem.
11. A gestão de riscos facilita a melhoria contínua da organização.
    - É necessário que as empresas e incluam estratégias para desenvolver a maturidade na gestão de riscos em todas as áreas da organização.

Torna-se evidente que a ABNT NBR ISO/IEC 31000 (2009) enxerga a Gestão de Riscos como ligada diretamente aos objetivos de um negócio. Esta norma preocupa-se de alinhar os conceitos de Estratégia e Risco e por isso deve ser pensada em todos os processos organizacionais. A ISO se preocupa em conscientizar as empresas de que o amadurecimento da empresa diante da Gestão de Risco é visto como um todo, embora para gerenciá-lo deve ser dividido em parcelas.

2.2 RISCOS

Mandarini (2005) definiu riscos como ameaças que manifestam probabilidade de ocorrência e com potencia para causar danos. Essas ameaças, segundo o autor, decorrem da falha humana, material, equipamentos ou da ação da natureza. A ABNT NBR ISO/IEC 31000 (2009), diz que a análise de riscos pode ser feita com uma variação gradativa de seus detalhes, dependendo do risco e de sua finalidade, diante dos dados e recursos disponíveis.

De acordo com Pressman (2004) a análise de risco é verdadeiramente um dos mais importantes passos para a administração de eventuais riscos, que possui como função quatro atividades distintas:

- Identificação dos riscos;
- Projeção dos riscos;
- Avaliação dos riscos;

- Gerenciamento e monitoração dos riscos.

A análise de risco é uma das análises cardeais que compõem esse estudo, sendo fundamental para o apontamento da vulnerabilidade e incerteza em uma organização, contribuindo assim na redução dos maiores problemas para o negócio.

2.2.1 Gestão de riscos.

Hopkin (2012) definiu a gestão de riscos como uma tomada de atitudes a partir daquilo que gera valor a organização, em outras palavras, as atividades para uma boa gestão virão diretamente de ações em busca dos melhores resultados possíveis reduzindo a volatilidade e as incertezas.

A ABNT NBR ISO/IEC 31000 (2009) define a gestão de risco como parte da tomada de decisão, tornando-se assim fundamental auxiliadora aos administradores para a escolha das melhores alternativas. A gestão de riscos tem como finalidade a priorização e distinção entre formas alternativas de ação. Ainda segundo a ABNT NBR ISO/IEC 31000 a gestão de riscos aborda explicitamente a incerteza, a fonte dessa incerteza, e como ela pode ser tratada.

Sendo assim a norma trata a gestão de risco como sistemática, estruturada e oportuna, o que garante resultados consistentes, comparáveis e confiáveis. Por isso a gestão de risco é totalmente baseada na coleta e tratamento das melhores informações disponíveis.

Para manter a confiabilidade dos dados a mesma norma ISO declara que a gestão de risco deve ser feitas sob medida, ou seja, sempre alinhada com o contexto interno de cada empresa e com o perfil equivalente a cada risco. A gestão de riscos irá então contemplar duas dimensões: humana e cultural. Sendo assim uma boa gestão de risco deve reconhecer as capacidades, percepções e intenções dos recursos humanos internos e externos - terceirização - que tem potencial para ajudar ou dificultar a execução dos objetivos traçados.

A gestão de risco por definição deve ser transparente e inclusiva. A transparência quer dizer que as partes interessadas devem ser consideradas

durante toda gestão, ao passo que a inclusão ocorre pela concessão de espaço para os recursos exporem suas ideias na determinação dos critérios de risco.

A capacidade de reagir a mudanças, conforme ocorrem eventos internos e externos, que por sua vez mudam naturalmente os cenários, faz com que surjam novos riscos. Portanto uma boa gestão de risco deve ser sensível a mudanças, percebendo-os e reagindo diante delas. Convém que as empresas, independente de seu porte, desenvolvam estratégias para melhoria gradativa de sua percepção de risco.

A gestão de risco é fundamental para o acontecimento da análise de risco, pois ela tem como missão gerenciar todas as atividades envolvidas a fim de aumentar as oportunidades e diminuir as chances de eventuais perdas.

2.2.1.1 Análise Qualitativa de Risco

O processo de levantamento de risco gera naturalmente uma lista imensa de riscos em potencial. Entretanto, segundo Dinsmore (2009) devido às limitações de tempo e recursos humanos, os riscos devem ser categorizados em diferentes níveis de importância, já que nem todos merecem o mesmo nível de atenção. Cria-se, portanto o desafio de priorizar os riscos que mereçam maior cuidado, para identificar os maiores desafios e suas respectivas soluções.

Segundo a definição que foi adotada neste trabalho, o risco possui duas características básicas probabilidade de ocorrência e com potencia para causar danos. O termo probabilidade é usado para a grau da incerteza, e o termo “potencia” designa o efeito direto nas tarefas. Segundo o mesmo autor, a analise de risco qualitativa enxerga essas duas dimensões usando classificações como "alta, média, baixa", definições que devem ser declaradas previamente num Plano da Gestão de Riscos. Assim a probabilidade do acontecimento dos riscos é avaliada ao mesmo tempo em que são avaliados os seus respectivos impactos.

O objetivo da análise de risco qualitativa é de estimar, através de uma série de critérios previamente acordados, os graus de criticidade em possíveis acontecimentos. Esse modelo é indicado para avaliar ativos intangíveis, contudo

essa avaliação pode ser subjetiva, porque depende diretamente do time de campo selecionado para execução do processo.

2.2.1.2 Análise Quantitativa de Risco

Dinsmore (2009) relata que a maioria dos riscos dos projetos ocorre em grupos, já que devido as dimensões desses os riscos ficam menos perceptíveis. A análise quantitativa de riscos se posiciona diante desses agrupamentos e encara cada risco de maneira individual, para que assim se torne clara a compreensão de cada um deles. Evidentemente a ação conjunta dos riscos exige naturalmente a análise de seu efeito combinado. Por isso existem inúmeros modelos de técnicas quantitativas, entre elas: análise de sensibilidade, árvores de decisão, Monte Carlo e a simulação de Monte Carlo.

A análise de risco quantitativa tem por missão calcular os valores objetivos de cada componente em seu impacto em caso de falha. A estimativa desses valores é levantada por meio de históricos de eventos anteriormente ocorridos, usando, por exemplo, os números de ocorrência, o custo de substituição e a perda da produtividade, entre outros.

Dentre os algoritmos que são indicados para esse cálculo, tomemos como exemplo a fórmula de Exposição de Perda Anual (ALE - *Annualized Loss Expectancy*), que segundo Peltier (2004) consiste na multiplicação do resultado da Expectativa de Perda Única (SLE - *Single Loss Expectancy*), pela Taxa de Ocorrência Anual (ARO - *Annualized Rate Occurence*)

A fórmula da Exposição de Perda Anual é:

Onde:

- EPA: Exposição de Perda Anual.
- EPU: Expectativa de Perda Única
- TOA: Taxa de Ocorrência Anual

O valor da Expectativa de Perda Única é obtido através da multiplicação do Valor do Ativo pelo Fator de Exposição. A formula da EPU é:

Onde:

- EPU: Expectativa de Perda Única
- VA: Valor do Ativo
- FE: Fator de Exposição

A representação do Valor de Exposição é dada pelo tamanho da perda ou impacto no valor de um ativo. A esse valor é atribuído um peso de 0 a 100%. O ARO é caracterizado pela frequência de uma ameaça se concretizar, em que o valor pode ser obtido pela tabela multiplicadora de perda anual, conforme apresentado na Tabela 2.

Tabela 2 - Tabela multiplicadora de perda anual

Tabela multiplicadora de perda anual		
Nunca		0,0
Uma vez em 300 anos	1/300	0,00333
Uma vez em 200 anos	1/200	0,005
Uma vez em 100 anos	1/100	0,01
Uma vez em 50 anos	1/50	0,02
Uma vez em 25 anos	1/25	0,04
Uma vez em 5 anos	1/5	0,20
Uma vez em 2 anos	½	0,50
Anualmente	1/1	1,0
Duas vezes ao ano	1/0,5	2,0
Uma vez ao mês	12/1	12,0
Uma vez por semana	52/1	52,0
Diariamente	365/1	365,0

Fonte: NETO, 2005, p. 24

2.3 METODOLOGIAS DE AVALIAÇÃO DE RISCO

As empresas têm necessitado cada vez mais de tecnologia, concomitantemente elas têm criado um vínculo de dependência nos seus processos com os recursos tecnológicos. Evidentemente a necessidade de mais tecnologia cria uma necessidade natural de se preparar para inconvenientes. Logo, compreender onde e como tratar os riscos tornou-se tarefa fundamental em qualquer empresa.

Para se obter resultados sólidos, consistentes e satisfatórios é necessário que a análise de risco se dê com organização e método. É neste ponto que a aplicação de uma metodologia de análise de risco torna-se obrigatória. A escolha de uma boa metodologia de Gerenciamento de Risco de TI, adequada às expectativas da organização, é essencial para o sucesso do gerenciamento de seu risco.

A seguir serão apresentadas as principais metodologias de gestão de risco em uso no mercado corporativo OCTAVE, FRAP, COBRA e COSO. É importante salientar que existem outras metodologias, como CRAMM, CORAS e *Risk Watch*, mas uma explicação exaustiva sobre estas foge ao escopo deste trabalho.

2.3.1 OCTAVE

A OCTAVE (2008), acrônimo de *Operationally Critical Threat, Asset and Vulnerability Evaluation*, é uma metodologia de análise de riscos desenvolvida por Christopher Alberts e Audrey Dorofee do Software Engineering Institute da Carnegie Mellon University. A metodologia começou a ser empregada nas organizações a partir do ano de 1999, com o propósito de identificar ativos, ameaças e vulnerabilidades existentes na infraestrutura da empresa (GARSON, 2009)

Coelho (2005) sublinha que a metodologia OCTAVE prioriza as áreas de melhorias para a organização, sendo aplicada de forma autodirigida, ou seja, possui uma equipe de análise interdisciplinar que fica responsável por identificar os ativos que estão expostos aos riscos.

O papel da metodologia é o de informar ou dar soluções de como se proteger dos riscos existentes no negócio, mediante a uma série de detalhes. O processo para aplicação da metodologia se divide em três fases:

1. Construir perfis de ameaças baseados nos ativos.
2. Identificar vulnerabilidades na infraestrutura.
3. Desenvolver planos de segurança

Na primeira fase, é feita a identificação de todo ativo para a organização, e consequentemente, é criado um perfil de ameaça para cada ativo crítico. Essa primeira fase se desenvolve dentro de quatro etapas, a saber:

1. **Ativos críticos:** são todos os pontos críticos, desde infraestrutura a recursos humanos da empresa, ou seja, tudo que apresenta relevância na continuidade das operações.
2. **Requerimento de segurança para os ativos críticos*:*** é onde ser realiza a identificação de cada ativo a ser protegido.
3. **Perfis de ameaças*:*** busca mostrar de forma estruturada as diferentes ameaças que se apresenta em cada ativo crítico.
4. **Práticas de segurança*:*** apresenta uma série de práticas de segurança visando prover soluções de como se prevenir das vulnerabilidades existentes.

Diante disto, conclui-se que as três primeiras etapas são ações de diferentes níveis da organização, e que a quarta é responsável por consolidar as etapas anteriores, verificando as informações fornecidas para indicar a melhor solução de segurança para cada uma delas.

A segunda fase da metodologia (identificar vulnerabilidades na infraestrutura) é onde ocorre a coleta de informações a serem analisadas pela equipe, de uma forma mais técnica, utilizando ferramentas para debilitar ações não permitidas sobre os ativos críticos da empresa.

Por último, a fase 3 (desenvolver planos de segurança) é onde são criadas estratégias de proteção e planos de mitigação para todos os riscos identificados, determinando assim, a melhor ação a ser tomada.

2.3.2 COSO

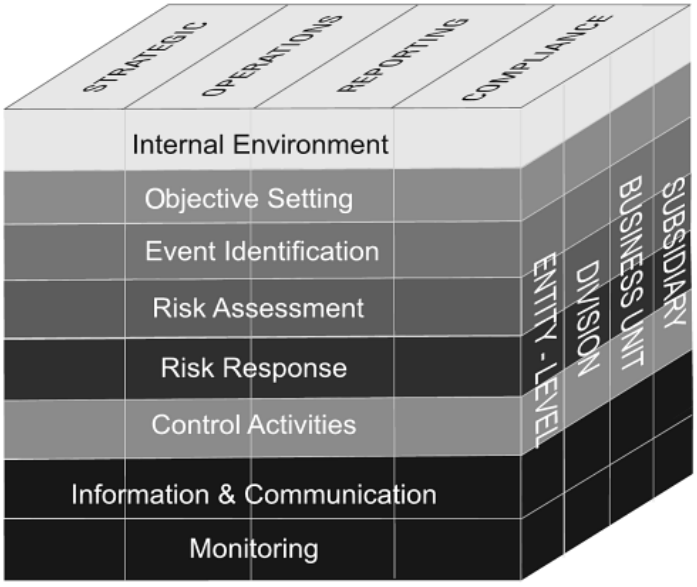
O COSO (1985), acrônimo de *Comittee of Sponsoring Organizations of the Treadway Commission* surgiu como um comitê convocado pelo congresso norte americano em resposta as irregularidades financeiras que ocorreram no final da década de 1980 (VAN GREUNING, 2009). O Comitê de Organizações Patrocinadoras da Comissão (COSO) formulou então uma estrutura de controle interno para auxiliar as organizações a garantir maior confiabilidade no alcance dos objetivos, reduzir o risco de perda nos ativos e promover a eficiência.

Ainda segundo Van Greuning (2009) a eficácia de um controle interno é medida a partir da capacidade de fornecer segurança razoável à administração e ao conselho da administração para a realização de seus objetivos em três aspectos:

1. Eficácia e eficiência das operações,
2. Confiabilidade dos relatórios financeiros e
3. Conformidade com as leis e regulamentos aplicáveis.

O foco da metodologia COSO está no reconhecimento da estrutura organizacional, ou seja, nas especificações das políticas de gestão, no relato real dos acontecimentos durante os processos e no cumprimento das regras. (Greuning, e Bratanovic , 2009)

Figura 1 - COSO - Enterprise Risk Management Framework



Fonte: Van Greuning (2009), p. 75

O controle interno definido pelo COSO consiste num conjunto coordenado de métodos para proteção do patrimônio, verificação da confiabilidade dos dados contábeis, promoção das políticas levantadas pela administração.

O COSO (2003) divide a gestão de riscos em oito componentes inter-relacionados, ilustrados na Figura 1. São eles:

- **Ambiente interno** – O ambiente interno inclui a filosofia da organização perante a gestão de risco.
- **Definição de objetivos –** Deve-se garantir que existe um processo de gestão corporativa para definir os objetivos e alinhá-los com a missão da entidade.
- **Identificação de Eventos** – Elenca os eventos, tanto internos quanto externos, que afetam o alcance dos objetivos.
- **Avaliação de Riscos –** Os riscos são analisados, considerando-se a potencialidade de ocorrência e seu impacto.
- **Resposta de Risco** – A gestão de risco selecionará possíveis respostas para cada cenário criado.
- **Atividades de Controle** - Conjunto de políticas e procedimentos que devem ser realizados para que os procedimentos adotados sejam efetivamente realizados.
- **Informação e comunicação –** Todas as informações relevantes são comunicadas durante qualquer estágio do COSO, evitando possíveis ruídos de comunicação.
- **Monitoramento –** Monitoramento constante de todos os processos e o replanejamento de execuções ou processos, caso seja necessário.

2.3.3 FRAP

A metodologia de processo de avaliação de risco FRAP (BIDGOLI, 2006), acrônimo de *Facilitated Risk Assessment Process,* foi desenvolvida por Thomas Peltier que ao perceber que a avaliação de riscos era encarada como uma grande tarefa, que exigia da organização uma contratação de um consultor especializado e poderia levar semanas a meses para ser concluído.

Nascia a necessidade do levantamento de riscos em menor tempo e sem dependência de fatores externos (PELTIER, 2005). A metodologia volta-se na aplicação de técnicas de gestão de risco de maneira eficaz em termos de custos. (FLAMINI, 2012)

A FRAP orienta que haja entre os recursos humanos pertinentes uma reunião de *brainstorm* para discutir riscos, vulnerabilidades e os danos em potencial, concomitantemente quando se avalia sobre a integridade, confidencialidade e disponibilidade dos dados. Com base nos dados levantados nesta reunião inicial são levantadas as ameaças e os riscos que devem ser priorizados.

A metodologia é puramente qualitativa, isto significa que ela não se preocupa de quantificar a probabilidade e magnitude dos riscos. Segundo Bidgoli (2006) a metodologia segue em três fases:

Primeira fase: reunião pré-FRAP

Os membros da equipe inicial são escolhidos sendo que geralmente a reunião contém de 7 a 15 membros. A equipe deve então determinar o escopo da reunião.

Nesta fase devem ser definidos o contexto e os objetivos que se pretende alcançar com essa investigação.

Os resultados dessa primeira fase são a identificação dos membros da equipe, a produção de um modelo visual do processo analisado e um conjunto das definições. Estas definições servirão para o resto dos processos, por isso a metodologia FRAP recomenda que a equipe presente na reunião concorde com nos seguintes pontos: integridade, confidencialidade, disponibilidade, risco, impacto, controle e vulnerabilidade, levantados na reunião.

Segunda fase:

A fase 2 é dividida em três partes:

A primeira parte é a estabilização da lógica que a reunião deve seguir: Aquele que deverá ser o líder de equipe, o que tomará as notas e etc...

Uma vez estabelecida a lógica que a reunião irá seguir, é verificado se todos os membros convocados para a reunião chegaram ao mesmo entendimento dos problemas que devem ser discutidos.

A terceira parte é o *brainstorming*. Nela os membros da equipe partilham o entendimento dos riscos que são importantes, na visão deles.

Terceira Fase:

A última etapa é a priorização onde os riscos elencados nas fases anteriores são classificados em duas dimensões:

Vulnerabilidade (baixo a alto) e impacto (baixo a alto).

2.3.4 COBRA

COBRA é o acrônimo de *Consultative, Objective and Bi-funetional Risk Analysis*, esse método foi criado em 1991 pela C&A Systems Security Ltda com o objetivo de fornecer as empresas meios para se auto avaliarem no âmbito de sua segurança, sem a necessidade de consulta a um recurso externo.

Segundo Botha (2008) a metodologia preocupa-se em fazer com que as empresas enxerguem sua segurança como uma questão de negócio, não como uma simples questão periférica de teor técnico - e que por consequência deve ser justificada em termos de custos e beneficio.

O COBRA é capaz de produzir uma análise de risco com cenários hipotéticos, através das respostas obtidas por um questionário feito no computador e recomendações para a ação, seguindo as diretrizes estabelecidas pela ISO/IEC 17799:2005 que trata da gestão de Segurança da Informação.

Este método usa a forma tradicional de consulta estruturada e avaliação continua em três etapas:

- Pesquisas de construção
- Avaliação de riscos
- Construção de relatórios.

Esta metodologia consiste em duas partes principais:

Consulta dos Riscos e Conformidade com a ISO.

Ambas as partes podem ser subpersonalidades, e se utilizarem de bases de conhecimento de especialistas.

Através da consulta dos riscos, o usuário tem a possibilidade de construir perguntas com base em *templates* e utilizar deles para construir conjuntos de respostas. As respostas podem ser alteradas posteriormente para comparar suas variações no impacto.

Segundo a ISO/IEC 17799 (2005), o COBRA pode produzir relatórios e propor recomendações com base nas melhores praticas.

A consulta de riscos por sua vez, expõe de forma breve por um levantamento dos tipos de ativos, vulnerabilidades, ameaças e controles através de um questionário.

Por isso a aplicação se preocupa com:

- Identificar as ameaças, vulnerabilidades e exposição do sistema;
- Mensurar o grau de risco real para cada área ou aspecto do sistema, e relacioná-lo diretamente ao potencial impacto nos negócios,
- Oferecer soluções e recomendações detalhadas a fim de reduzir os riscos.
- Gerar relatórios técnicos e executivos.

Fonte: RISKWORLD, 2012.

Como a metodologia trabalha:

Figura 2 - O modelo de avaliação de risco COBRA

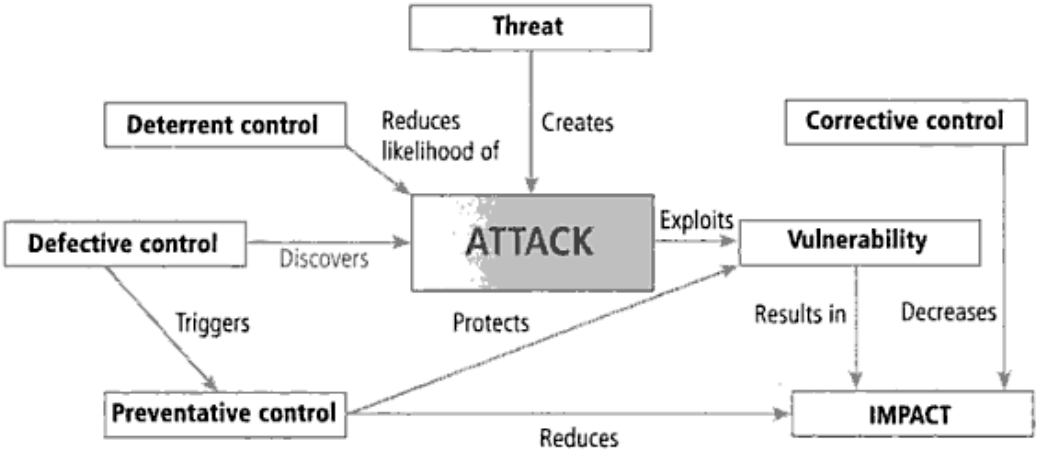


Figure 6.4 The COBRA risk evaluation model
Source: The Security Risk Analysis Directory, 2003.

Fonte: Botha (2008), p. 121

A metodologia enxerga que toda ameaça cria naturalmente um ataque e acaba por resultar em um impacto. Para que os riscos sejam reduzidos é necessário o uso de controles corretivos para redução de seu respectivo impacto.

2.4 SOLUÇÃO ESCOLHIDA:

De modo geral os aspectos das metodologias analisadas – COSO, FRAP, COBRA e OCTAVE – apresentaram uma capacidade de suporte para o objetivo proposto por este trabalho, porém, considera-se que cada organização dentro de seu perfil, possui exiguidades à serem trabalhadas.

Neste estudo de caso, foram atribuídos dois critérios para escolha da metodologia - maturidade e recursos. Deve-se entender por maturidade o conhecimento organizacional dos recursos perante aos processos internos e entende-se por recursos, a quantidade de profissionais atuantes na área de TI.

2.5 A SITUAÇÃO DA IOL PERANTE A MATURIDADE E RECURSOS:

Em quesito de maturidade, de acordo com a entrevista com o representante da IOL, a empresa encontra-se com baixa difusão do conhecimento entre seus colaboradores. Já seu número de recursos humanos é de apenas 8 colabores.

A IOL não possui conhecimento das resoluções amplamente difundidas entre seus colaboradores, no entanto, ao ocorrer eventualidades os colaboradores contam com um serviço interno de base de conhecimento para procurar por possíveis soluções.

Portanto, a escolha da metodologia se deu diante da verificação da necessidade em enquadrar-se ao nível de conhecimento e de recursos que ela possui.

2.5.1 COSO

O modelo COSO é destinado a empresas que desejam melhorar os controles internos e seus relatórios financeiros. Para a implantação de uma análise de risco segundo a metodologia COSO é necessário o conhecimento detalhado do ambiente interno e externo da organização, principalmente da filosofia organizacional e os eventos no meio desta. Neste contexto a metodologia apresenta-se como indicada somente a instituições que conheçam bem seus processos, entretanto a IOL não possuí no seu time de colaboradores, recursos que conheçam detalhadamente os processos.

2.5.2 FRAP

O método FRAP tem como proposta a resolução de problemas que são abertamente conhecidos pelos colaboradores, através de reuniões de *brainstorm*. Embora a um primeiro olhar o modelo seja entusiasmante, esse método exige o conhecimento técnico de todos colaboradores presentes na reunião. O modelo também exige uma equipe razoavelmente grande, já que as reuniões devem

preferencialmente ser feitas por 7 à 15 membros. No entanto o número de recursos da IOL é de oito membros e seus colaboradores não possuem um grande conhecimento técnico.

2.5.3 COBRA

A Metodologia COBRA funciona através de um questionário eletrônico para adequar a organização as normas prescritas pela ISO/IEC 17799, que trata da segurança da informação. Sendo assim, para sua aplicação, é necessário que os funcionários tenham um alto nível de conhecimento sobre as partes técnicas da empresa, pois o questionário não possui *feedback* da confiabilidade dos dados imputados.

2.5.4 OCTAVE

A metodologia OCTAVE é focada diretamente na mitigação dos riscos da organização e informa soluções de como evitá-los de forma que não impacte nos ativos da organização. Ela se enquadra em vários níveis empresariais e desenvolve uma análise de como evitar riscos em todos os pontos críticos da organização. O OCTAVE tem como proposta ser guiado por membros que não possuem conhecimento técnico dos processos e por equipes de qualquer magnitude.

Diante desta análise, é perceptível que o método que melhor se enquadra com o perfil da IOL - que não possui o conhecimento técnico amplamente difundido com seus colaboradores - é a metodologia OCTAVE, que por sua vez tem o papel de mitigar os riscos, no que se denomina de extrema importância para a funcionalidade dos ativos do negócio, se preocupando com a falta de conhecimento técnico de seus colaboradores.

Devemos considerar que cada organização, cada qual dentro de seu perfil, possui exiguidades a serem trabalhadas. Nesse estudo de caso foram atribuídos dois critérios para escolha da metodologia: maturidade e recursos. Deve-se entender por maturidade o conhecimento organizacional dos recursos perante os

processos internos e entende-se por recursos os profissionais atuantes na área de TI.

O método OCTAVE define requisitos para segurança da informação, através da avaliação dos riscos sobre ameaças dos ativos críticos da organização. Sendo assim, a metodologia tem o papel de identificar, priorizar e gerenciar os riscos, por meio de várias ferramentas, técnicas e métodos analisados.

Conforme Alberts e Dorofee (2003) essa metodologia é flexível, adaptando-se assim a qualquer nível e tipo de organização.

2.5.4.1 Princípios

Os conceitos levantados são o cerne da análise e avaliação de riscos, proporcionando, assim, uma base para o processo de avaliação. Diante disto, a metodologia se organiza em três áreas:

- **Princípios de Avaliação de Risco na Segurança da Informação:**
  Contemplando os aspectos fundamentais que abordam a informação na avaliação de risco de segurança. Seus principais pontos são:
  - Auto direção – Os colaboradores da organização se responsabilizam pelo controle e gerenciamento da análise de risco;
  - Medidas adaptáveis – As medidas devem ser flexíveis, de forma que se adaptem a qualquer mudança que possam surgir futuramente;
  - Processo definido – A necessidade constante de seguir padrões e procedimentos definidos e
  - Base para um processo contínuo – Melhora e acompanhamento constante do nível de segurança, é executado estratégias e planos de segurança para serem cumpridas em determinado tempo.

- **Princípios de Gestão de Riscos:**

  Aborda a visão prospectiva, pontos críticos e a gestão integrada, ou seja, os princípios básicos para mostrar a gestão de risco de forma eficaz. Deve-se entender por:

- Visão prospectiva – A visão sobre os ativos mais críticos da organização;
- Pontos críticos – Este princípio complementa a visão prospectiva, com o objetivo de focar nos ativos críticos; (E)
- Gestão integrada – As políticas e estratégias da segurança devem ser fiéis as políticas e as estratégias organizacionais.

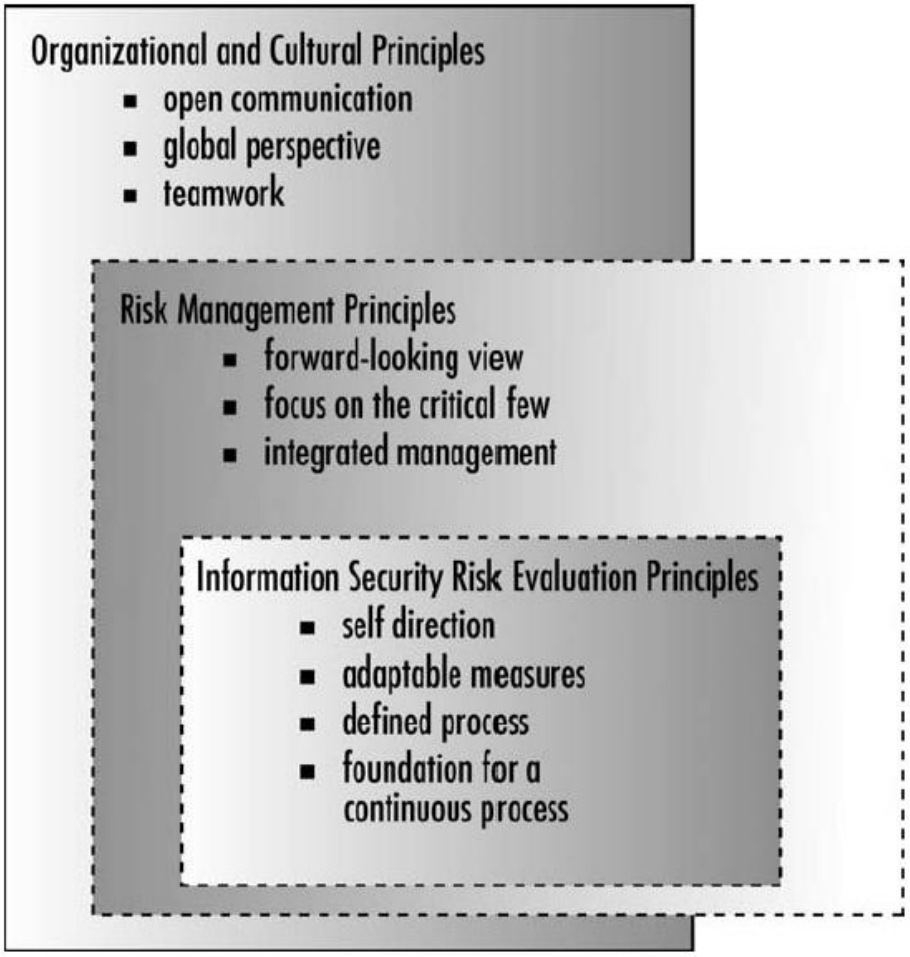
- **Princípios Organizacionais e Culturais:**

A preocupação com a união dos aspectos da organização com sua cultura, que são primordiais para os melhores resultados da gestão de riscos no negócio.

- Comunicação aberta – Um bom diálogo pra um melhor entendimento dos problemas da empresa;
- Perspectiva global – Os colaboradores devem criar uma visão geral sobre os ativos da organização;
- Trabalho em equipe – Para elevação do nível de segurança é necessário que as atividades se realizem de forma coletiva.

A relação desses tópicos pode ser demonstrada através do seguinte esquema:

Figura 3 - Princípios e atributos da Avaliação de Risco da Segurança da Informação



Fonte: Alberts e Dorofee, 2003, p. 20.

2.5.4.2 ESTRUTURA

O OCTAVE busca obter informação detalhada, sistemática e com o contexto direcionado, procurando assim ajudar a empresa a melhorar sua segurança da informação.

Para a condução dos processos de Gestão de Risco o OCTAVE recomenda que se tenha uma equipe de análise, dividida em dois grupos: o primeiro com pessoas da área de negócio e o segundo com colaboradores da área de TI (OCTAVE, 2001). Os dois grupos são vitais para que ocorra uma visão global dos riscos, envolvendo toda a organização. Os objetivos da equipe de análise são:

- Identificar os recursos de informação que são importantes para a organização (os ativos).

- Focar as atividades de análise nos recursos considerados críticos.

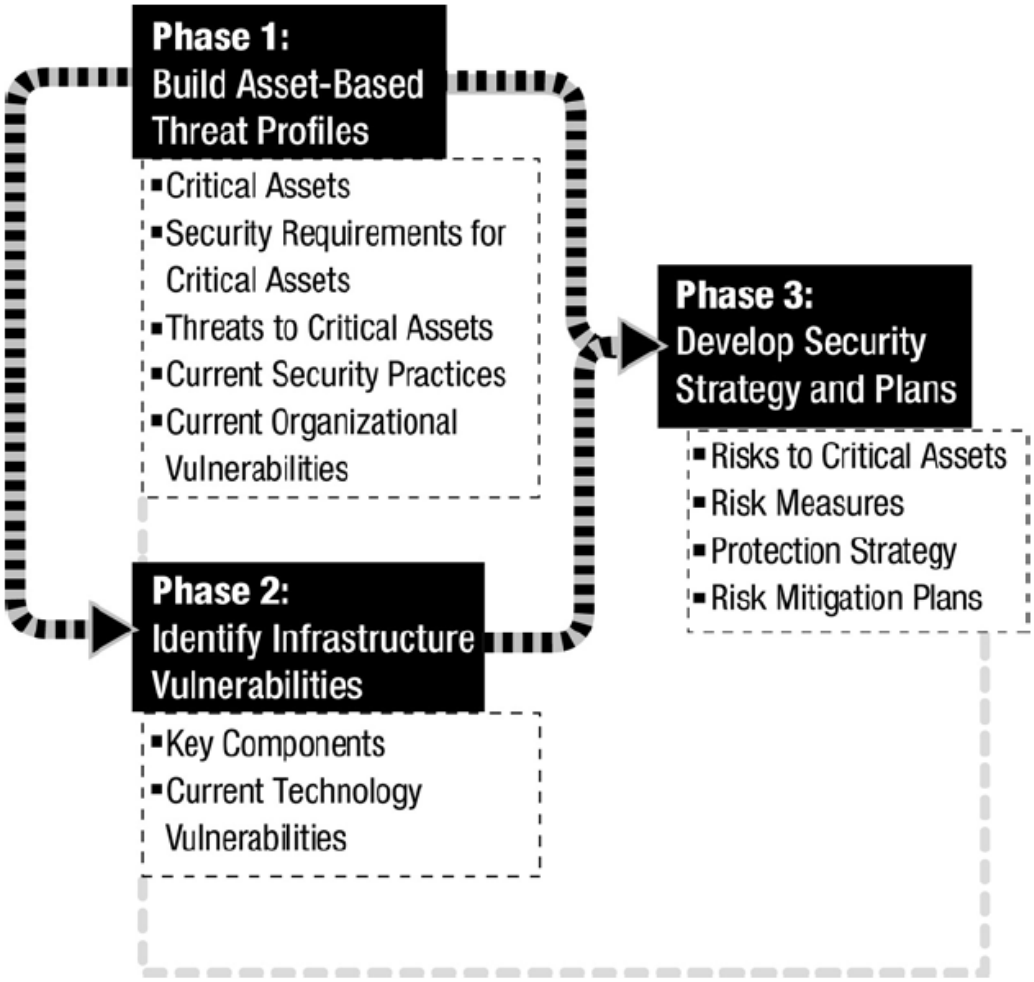
Para esta análise é importante que a equipe considere os relacionamentos entre os ativos e as ameaças a que estão expostos, além de vulnerabilidades, que podem aumentar a exposição destes ativos.

O OCTAVE permite analisar e avaliar os riscos no contexto operacional, isto é, ele mapeia como os sistemas são usados, buscando assim alinhar os objetivos de negócio com os requisitos de segurança. A metodologia entende que para a organização conseguir atingir seus objetivos, TI e os colaboradores deve estar alinhados com eles. Ou seja, para que a organização consiga atingir suas metas, os colaboradores precisam compreender quais recursos relacionados à informação são importantes e como devem ser protegidos.

2.5.4.3 Fases do OCTAVE

O método OCTAVE detalha três fases que apresentam aspectos organizacionais, tecnológicos e de avaliação dos riscos. A Figura 4 (a seguir) ilustra claramente a estrutura das três fases e os seus respectivos acessos principais.

Figura 4 - Fases OCTAVE



Fonte: Alberts e Dorofee, 2011.

A seguir, cada uma das fases é mais extensamente detalhada.

FASE 1: Construir perfis de ameaças para os ativos críticos

A primeira fase está relacionada aos aspectos organizacionais. Seu foco é direcionado nas ameaças existentes na empresa e na classificação de cada ativo por sua maior importância, onde serão selecionados colaboradores da própria organização, para atuarem no levantamento dos ativos que são importantes para a empresa, demonstrando também a forma que esses eles são protegidos. Essas informações serão consolidadas e feita uma escolha do que é mais impactante para

alcançar a missão e os objetivos almejados pela organização, feito um mapeamento das necessidades de segurança para cada ativo crítico, assim, criando um perfil de ameaça para cada um deles.

Para compreender seus processos é importante conhecer o funcionamento dos:

- Ativos críticos: Levantar todos os ativos que apresentam maior criticidade para a continuidade do negócio;
- Requisitos de segurança para os ativos críticos: Identificar as questões de maior importância para poder protegê-las contra possíveis ameaças;
- Ameaças para ativos críticos: Identificar de maneira estruturada as ameaças existentes em cada ativo crítico, verificando o impacto que possa gerar caso elas ocorram.
- Práticas atuais de segurança: Desenvolvimento de estratégias para proteção dos ativos críticos, através de ferramentas que auxiliam na compreensão do porque da vulnerabilidade.

FASE 2: Identificar as vulnerabilidades da infraestrutura

Nesta fase é avaliada a infraestrutura tecnológica da empresa. Sendo definida pela equipe de análise a identificação dos componentes relacionados aos ativos críticos, buscando fraquezas que podem levar a uma ação não autorizada. Tratando todos os ativos críticos a ameaças levantados na primeira fase, e em seguida a realização de testes de vulnerabilidade para cada um deles, reconhecendo onde estão as possíveis vulnerabilidades.

Com os componentes já testados, é discutido entre a equipe o porquê tais ativos estão vulneráveis, a forma que eles afetam e qual ação devem ser tomadas. As saídas desta fase constituem em:

- Componentes chaves: Os componentes principais se relacionam com os ativos críticos, a fim de mostrar por onde eles estão sendo ameaçados.
- Vulnerabilidades tecnológicas atuais: Consiste numa atividade puramente técnica que utiliza ferramentas para detecção das vulnerabilidades existentes.

FASE 3: Desenvolver planos estratégicos e de segurança

Nesta fase a equipe age sobre os riscos identificados, estabelecendo soluções para cada um deles e criando estratégias para mitigá-los. O resultado dessa fase é uma análise de impacto das ameaças sobre os ativos críticos e o desenvolvimento de critérios para avaliação dos riscos, através da criação de um perfil de criticidade.

Tendo como saída o levantamento dos Riscos para ativos críticos, onde eles são definidos baseando-se nos perfis de ameaças identificados nas fases anteriores nos seguintes critérios:

- Medidas do risco: Medindo a escala do risco, sendo classificado como alto, médio ou baixo.
- Estratégias de proteção: É feito um plano estratégico de proteção e mitigação dos riscos para a organização.
- Planos de mitigação dos riscos: É desenvolvido um plano de melhoria para a proteção dos ativos críticos, para que assim, seja implementado os resultados de avaliação analisados nas fases anteriores.

3 A EMPRESA

A empresa Itapecerica Online Telecomunicações e Informática Ltda. situada na região de Itapecerica da Serra, é um provedor de internet que opera há 14 anos no mercado, fundada em 03/08/1998. O serviço de internet disponibilizado é conhecido como WipLink, Banda Larga via Rádio, que oferece conectividade para qualquer perfil de cliente, tais como:

- Residências
- Condomínios
- Pequenas, médias e grandes empresas.
- Links dedicados ponto-a-ponto

Em meados de 2008, a IOL concluiu sua reestruturação e licença SCM da ANATEL para poder operar em nível nacional nos mercados de Banda Larga Corporativa, Clear Channel, Hosting, Voip e soluções integradas de TI.

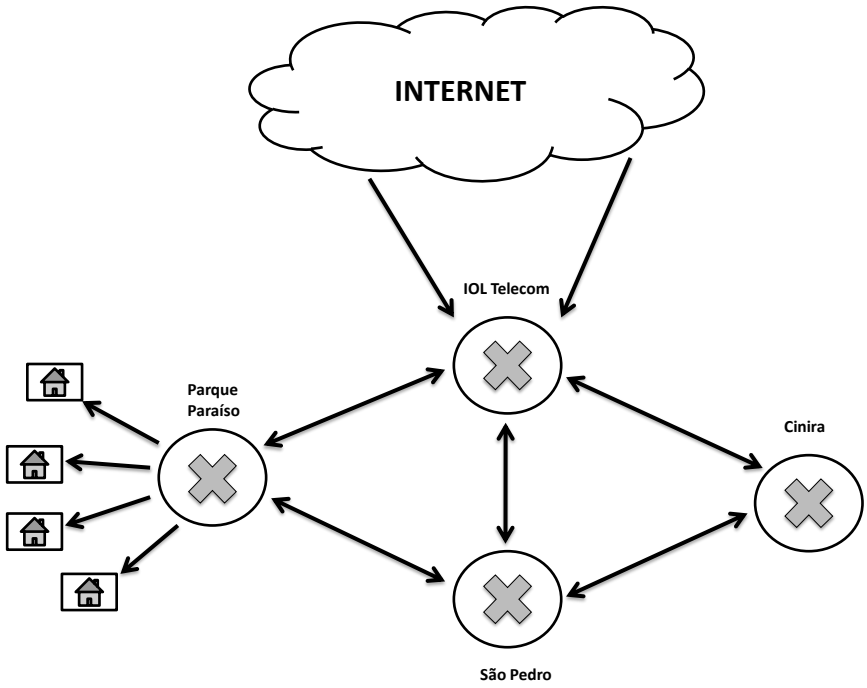
Com parcerias estratégicas, além de fornecer banda larga por wireless, fornece também acesso fibra ótica e par metálico, onde sua estrutura própria não tem abrangência. As parcerias também possibilitam o oferecimento de serviços de telefonia fixa-STFC com portabilidade numérica e serviços de PABX digital como: secretária eletrônica, desvio de chamadas e gravações de ligações.

No âmbito de rede internet, a IOL é um ASN independente reconhecido pelo LACNIC e NIC.Br e seu backbone redundante é atendido por links profissionais de alta performance, possibilitando um rápido crescimento com as demandas dos seus serviços e mantendo altos níveis de disponibilidade de serviços.

3.1 TOPOLOGIA

O layout físico da topologia de rede da IOL possui suas antenas principais em três bairros da região de Itapecerica da Serra, sendo, Parque Paraíso, São Pedro e Cinira. Todas essas antenas conversam entre si, para garantir alta porcentagem de funcionamento, pois quando ocorre algum problema em uma das rotas, o protocolo utilizado pela IOL, o OSPF, se encarrega de identificar as rotas operantes e indicar o menor caminho para a rede.

Figura 5 - Topologia lógica da infraestrutura da IOL



FONTE: Elaborado pelo autor

3.2 ESCOLHA E JUSTIFICATIVA

A IOL foi escolhida por que além de ser uma empresa conhecida por um dos autores desta monografia ela também não possui seus riscos mapeados, de forma que fica evidente diante das razões já mencionadas a necessidade de conhecê-los e mapeá-los.

3.3 PERSPECTIVAS

A estrutura de backbone da IOL abrange repetidoras em São Paulo, Taboão da Serra, Embú e Cotia. Ela firma novas parcerias comerciais que permitirão para a empresa uma atuação mais agressiva no fornecimento de links profissionais na maioria das grandes cidades do Brasil. Em relação à telefonia fixa, seu objetivo é oferecer um custo inferior ao praticado normalmente pelas grandes companhias de telefonia.

O sistema administrativo integrado com a infraestrutura técnica e gerenciamento financeiro possibilitam um melhor controle dos clientes, permitindo um crescimento acelerado, devido à centralização e fácil operação.

Novas tecnologias estão sempre sendo avaliadas para oferecer a melhor solução para os seus clientes e acompanhando o desenvolvimento tecnológico do segmento.

4 CONTROLES PARA A MITIGAÇÃO DOS RISCOS

Para atender aos objetivos desta monografia de estabelecer diretrizes e princípios gerais de implementação, manutenção e melhora da gestão da segurança da informação em uma empresa de prestação de serviços de acesso à Internet, um conjunto de controles, obtidos a partir da NBR ISO/IEC 17799 (2005) foi escolhido. Este conjunto de controles será utilizado no Capítulo 5, para demonstrar ações que podem ser tomadas visando a diminuição dos riscos.

Os controles aqui apresentados estão agrupados em 7 áreas, a saber:

- Gestão de Conhecimento
- Gestão de Pessoas
- Gestão de Desempenho
- Gestão de Relacionamento
- Gestão de Tecnologia
- Gestão de Ameaças
- Práticas de Contrato

Os controles de cada um destes grupos estão descritos nas seções a seguir.

4.1 GESTÃO DE CONHECIMENTO:

4.1.1 Política de Segurança da Informação

É fundamental para organização conhecer onde estão seus riscos. A norma estabelece três princípios para conhecê-los.

I. É realizado um levantamento através da análise/avaliação de riscos, levando em conta os objetivos e estratégias de negócio para empresa.
II. É considerado todo ambiente interno e externo, desde cláusulas contratuais às regulamentações governamentais.
III. São considerados os princípios, objetivos, requisitos do negócio.

4.1.2 Treinamento de Pessoal

Convém que os funcionários da empresa, quando pertinente, recebam treinamentos apropriados para conscientização, e continua atualização perante as políticas organizacionais.

4.1.3 Compartilhamento de Conhecimento

É necessária a existência de controles apropriados que auxiliem no gerenciamento e compartilhamento de informações.

4.2 GESTÃO DE PESSOAS

4.2.1 Papéis e Responsabilidades

Para que a política de segurança da informação da organização seja respeitada, é necessário definir e documentar papéis e responsabilidades para segurança da informação de funcionários, fornecedores e terceiros.

4.2.2 Assegurar a conformidade de responsabilidade

Conscientizar os funcionários, fornecedores e terceiros sobre as ameaças existentes na segurança da informação e assegurá-los sobre suas responsabilidades e obrigações na organização, respeitando sempre a política de segurança da informação durante sua atuação na empresa, diminuindo assim, o risco de erro humano.

4.3 GESTÃO DE DESEMPENHO

4.3.1 Monitoramento do uso do sistema

Criar procedimentos para monitorar os recursos de processamento da informação, para que com os resultados obtidos seja realizada uma análise crítica regularizada.

4.3.2 Identificar e implementar melhorias de desempenho

É necessária a definição de critérios para verificação eficaz desempenho e monitoração de registro.

4.4 GESTÃO DE RELACIONAMENTO

4.4.1 Seleção de Provedor de Serviços

Convém que sejam pré-acordados contatos apropriados com os prestadores de serviço de informação, de forma que sejam garantidas ações adequadas em caso de incidentes de segurança.

4.4.2 Revogação dos direitos

A organização deve possuir o direito de monitorar e revogar as atividades dos usuários; bem como a de manuseio de equipamentos quando as atividades cessarem.

4.5 GESTÃO DE TECNOLOGIA

4.5.1 Manutenção de disponibilidade do ativo

É necessário garantir que os usuários autorizados tenham acesso aos ativos, sempre que necessário.

4.5.2 Continuidade dos Serviços

Convém que a política possua um gestor responsável pela manutenção e análise dos ativos.

4.5.3 Entrega do Serviço

Convém que as áreas de segurança sejam restringidas com controles de acesso de entrada apropriados.

4.6 GESTÃO DE AMEAÇAS

4.6.1 Política de Controle de Acesso

A política de controle de acesso estabelecida deve ser documentada e analisada de forma crítica, baseando-se nos requisitos de acesso e na segurança da informação do negócio.

4.6.2 Riscos causados por colaboradores

Convém que haja controles para não vazamento de informações relevantes da empresa.

4.7 PRÁTICAS DE CONTRATO

4.7.1 Estabelecimento de contrato

Os regulamentos contratuais devem ser definidos de forma explicita, documentada e sempre atualizada para todos os sistemas de informação da empresa.

4.7.2 Acordo de níveis de serviços

Convém que haja acordos formais entre os fornecedores de serviço e cliente.

4.7.3 Acordo de confidencialidade

Convém que o compartilhamento de informações seja restrito para garantir que essas não sejam repassadas a pessoas não autorizadas.

4.7.4 Condições de contratação

Como obrigação convém que os colaboradores, fornecedores e terceiros concordem e assinem um contrato que declare seus papeis e responsabilidades.

5 ESTUDO DE CASO

O estudo de caso foi desenvolvido na empresa IOL. Os principais processos da empresa foram analisados e uma entrevista estruturada foi conduzida com o principal sócio da empresa.

Para que se pudesse mapear os riscos da empresa, um processo formal de Análise de Risco, seguindo a metodologia OCTAVE, descrita no Capítulo 3 foi conduzido. Esta fase procurou analisar os processos envolvidos na operação da empresa. Nas seções a seguir descreve-se cada uma das etapas do processo de análise de risco em conformidade com a metodologia escolhida.

5.1 IDENTIFICAÇÃO DOS RISCOS

Com base no entendimento da operação da empresa IOL foram identificados os riscos aos quais a organização está suscetível. As tabelas abaixo apresentam os resultados obtidos a partir da análise de risco.

Tabela 3 - Risco 1

Link Internet	
Tipo de Ameaça	Problemas de Segurança para o link de Internet
Falha no link	Interrupção - O link de internet é o ponto de comunicação entre a empresa e seus clientes, sem essa conexão não seria possível prestar os serviços aos clientes, causando a insatisfação dos mesmos.

FONTE: Elaborado pelo autor

Tabela 4 - Risco 2

Roteador	
Tipo de Ameaça	Problemas de Segurança para o roteador
Falha do equipamento	Interrupção - O roteador é um equipamento que permite o envio de sinal para outras redes, sendo assim é primordial o seu funcionamento, pois sem essa comunicação entre os computadores os clientes ficariam sem o acesso a internet.

FONTE: Elaborado pelo autor

Tabela 5 - Risco 3

Funcionários	
Tipo de Ameaça	Problemas de Segurança para a ausência de funcionários
Ausência por diversos motivos	Ausência - Porque o conhecimento por não ser difundido, fica a mercê dos funcionários e na ausência dos mesmos o serviço não seria realizado.

FONTE: Elaborado pelo autor

Tabela 6 - Risco 4

Energia Elétrica	
Tipo de Ameaça	Problemas de Segurança para a ausência de energia elétrica
Ausência	Ausência - A empresa possui gerador que funciona por até 10 horas contínuas.

FONTE: Elaborado pelo autor

Tabela 7 - Risco 5

Backup	
Tipo de Ameaça	Problemas de Segurança para o backup
Perda de dados importantes	Perda - Backup é uma cópia dos dados da empresa, sendo assim é fundamental a sua realização caso aconteça algum problema, como perda, pois ele dá a chance de recuperá-los. Então caso esse processo não seja realizado a organização não teria como saber o histórico do que foi perdido ou não.

FONTE: Elaborado pelo autor

Tabela 8 - Risco 6

Contratos	
Tipo de Ameaça	Problemas de Segurança para os contratos
Desentendimentos com clientes Perda de documentação	Desentendimentos com clientes - Sem base documental não há como discutir juridicamente. A ruptura de contrato pode gerar uma série de danos.

FONTE: Elaborado pelo autor

Tabela 9 - Risco 7

Gerador	
Tipo de Ameaça	Problemas de Segurança para a ausência de energia elétrica
Falha de funcionamento	Interrupção - Porque na falta de energia, por exemplo, nada funcionaria.

FONTE: Elaborado pelo autor

5.2 AVALIAÇÃO DOS RISCOS

Nesta etapa, com base no processo da fase anterior, é possível analisar o impacto que os ativos críticos podem sofrer. Esta análise é apresentada nas Tabelas abaixo.

Tabela 10 – Avaliação de Risco 1

Ativo	Resultado	Descrição do impacto	Valores
Link Internet	Interrupção	Clientes sem internet	Alto

FONTE: Elaborado pelo autor

Tabela 11 - Avaliação de Risco 2

Ativo	Resultado	Descrição do impacto	Valores
Roteador	Interrupção	Clientes sem internet	Alto

FONTE: Elaborado pelo autor

Tabela 12 - Avaliação de Risco 3

Ativo	Resultado	Descrição do impacto	Valores
Funcionários	Ausência	Não realização de instalação do serviço	Médio

FONTE: Elaborado pelo autor

Tabela 13 - Avaliação de Risco 4

Ativo	Resultado	Descrição do impacto	Valores
Energia Elétrica	Ausência	Não possui devido ao gerador.	Baixo

FONTE: Elaborado pelo autor

Tabela 14 - Avaliação de Risco 5

Ativo	Resultado	Descrição do impacto	Valores
Backup	Perda de dados	Perda de informações	Médio

FONTE: Elaborado pelo autor

Tabela 15 - Avaliação de Risco 6

Ativo	Resultado	Descrição do impacto	Valores
Contratos	Ruptura	Perda de cliente	Médio

FONTE: Elaborado pelo autor

Tabela 16 - Avaliação de Risco 7

Ativo	Resultado	Descrição do impacto	Valores
Gerador	Interrupção	Na ausência de energia nada funcionaria.	Alto

FONTE: Elaborado pelo autor

5.3 TRATAMENTO DOS RISCOS

Nesta fase acontece o tratamento dos riscos identificados e avaliados nas seções anteriores. Os riscos foram tratados usando-se o conjunto de controles apresentados no Capítulo 4, visando assim mitigá-los de maneira efetiva. A seguir, os controles escolhidos para serem implementados para cada risco identificado são apresentados.

Ativo: Link Internet

Ameaça: Interrupção

Controle a ser implementado:

4.7.2 - Acordo de Nível de Serviço

Conforme determina o controle 4.7.2 qualquer serviço que é provido necessita de uma formalização contratual para acordar o nível do serviço que deve ser disponibilizado. Por exemplo, ao contratar o serviço de internet da empresa “A” é documentado e pactuado junto ao cliente que o serviço terá X% de sinal disponível, neste mesmo contrato é definida uma multa prevendo a possível não realização dessa clausula, encarando-a como quebra contratual. Fica evidente através do exemplo que a empresa “A” terá a obrigação legal de pagar uma multa, pois tudo foi previamente regido no contrato. De forma análoga ao exemplo, a IOL para garantir o seu serviço precisa de um Acordo de Nível de Serviço (ANS) para que caso ocorra problemas similares – previstos contratualmente – ela tenha um plano para não infringir as clausulas do contrato e assim resolver o problema o mais rápido possível, cumprindo o tempo determinado no contrato.

Ativo: Roteador

Ameaça: Interrupção

Controle a ser implementado:

4.5.2 - Continuidade dos Serviços

Conforme abordado no controle 4.5.2, para que a organização se prepare diante de riscos a esse ativo – que é considerado como principal ativo da empresa – com a contratação ou designação de um gestor responsável pela manutenção e análise desse ativo.

Ativo: Funcionário

Ameaça: Ausência

Controles a serem implementados:

4.2.2 - Assegurar a conformidade de responsabilidade

4.1.3 - Compartilhamento de Conhecimento

Diante do controle 4.2.2 convém a organização que seus colaboradores estejam conscientizados sobre suas responsabilidades e deveres diante das políticas organizacionais. Concomitantemente a esse procedimento, é necessário que o ambiente de trabalho propicie aos funcionários a possibilidade de integração e compartilhamento dos conhecimentos adquiridos, conforme o controle 4.1.3 sugere.

Ativo: Energia Elétrica

Ameaça: Ausência

Controle a ser implementado:

4.4.1 Seleção de Provedor de Serviços

O risco a este ativo existe num cenário com ausência de energia por mais de 10 horas contínuas. Caso este cenário venha ocorrer é necessário que esteja previamente acordada uma garantia junto à concessionária de energia para o refornecimento do serviço, conforme sugerido no controle 4.4.1.

Ativo: Backup

Ameaça: Perca de dados

Controle a ser implementado:

4.3.2 Identificar e implementar melhorias de desempenho

Conforme indicado pelo controle 4.3.2 é necessário que haja critérios definidos para realização do backup em serviços que estejam em distâncias físicas consideráveis, através de uma monitoração constante dos registros da empresa.

Ativo: Contratos

Ameaça: Desentendimento com o cliente

Controle a ser implementado:

4.7.1 Estabelecimento de contrato

É necessário que os contratos estejam devidamente atualizados e promulgados junto aos clientes, como trata o controle 4.7.1, evitando maiores transtornos na relação da organização com seus clientes.

Ativo: Gerador

Ameaça: Falha no equipamento

Controle a ser implementado:

4.5.2 Continuidade dos Serviços

Conforme abordado no controle 4.5.2, para que a organização se prepare diante de riscos a esse ativo é necessária à contratação ou designação de um gestor responsável pela manutenção e análise desse ativo.

6 CONSIDERAÇÕES FINAIS

Este trabalho abordou um estudo de caso na IOL com uma análise de risco. O principal objetivo desse TCC foi a identificação e proposta de tratamento dos riscos da empresa. Para isso, inicialmente realizou-se um árduo processo de estudo das principais metodologias de avaliação, levantamento e tratamento de risco existentes. Dentre as diversas metodologias existente, optou-se pelo estudo das 4 mais utilizadas: COSO, FRAP, COBRA e OCTAVE.

Realizou-se então uma pré-análise junto à organização para que se pudesse conhecer seu ambiente, filosofia e estrutura. Os resultados desta fase permitiram a identificação das peculiaridades e características que guiaram a escolha do método mais adequado às suas necessidades: o OCTAVE. Essa escolha usou dois pilares como critérios de escolha: maturidade e recursos.

Uma vez escolhida, partiu-se para um planejamento para a aplicação da metodologia. A partir da coleta inicial dos dados e do entendimento da metodologia, foi realizada uma entrevista estruturada com a alta administração da empresa, utilizando-se o questionário presente no Anexo A. Após esta fase e seguindo a metodologia, realizou-se a identificação e análise dos riscos através de três fases distintas:

1. Construir perfis de ameaças para os ativos críticos;
2. Identificar as vulnerabilidades da infraestrutura;
3. Desenvolver planos estratégicos e de segurança.

Nesta fase, foi preciso vencer diversas dificuldades encontradas, especialmente cruzar a fronteira linguística e a seleção criteriosa de conteúdo, que embora possua muitas fontes, enfrenta limitações em número de autores que são especialistas. Dificuldades essas que foram ultrapassadas com a persistência e uma escolha seletiva das fontes a qual se deveria confiar.

O fruto direto da aplicação da metodologia foi tornar mais claro os pontos mais obscuros dos riscos e como prevenir os efeitos diretos dos acontecimentos extraordinários causados por eles. Esse levantamento foi inédito na história da IOL, e através dele a organização pôde conhecer onde estão e como tratar seus riscos.

Evidentemente a análise de risco é continua e deve ser periodicamente atualizada, por isso o presente trabalho, embora tenha alcançado êxito em sua proposta inicial, deixou como herança a necessidade de revisão continua da análise nos processos organizacionais, legado esse que deve ser continuado.

6.1 TRABALHOS FUTUROS:

Com base no trabalho realizado, fica evidente a necessidade do desenvolvimento de forma contínua e periódica para revisão da confiabilidade dos dados e descoberta de possíveis mutações no comportamento das já identificadas.

Dessa forma, novas análises devem ser feitas para validar os dados já pré-identificados e conhecer as mutações que ocorrerem na organização.

REFERÊNCIAS

ALBERTS, Christopher e DOROFEE, Audrey. **Managing Information Security Risks: The Octave Approach**. Boston.Addison Wesley, Inc. 2003.

ALBERTS, Christopher e DOROFEE, Audrey. **OCTAVE Threat Profiles**. Disponível em http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf. Acesso em: 07 nov 2012.

ALBERTS, Christopher e DOROFEE, Audrey. **OCTAVE^{SM} Criteria, Version 2.0.** Pittsburgh, PA. Carnegie Mellon University. 2001

BIDGOLI, Hossein. **Handbook of Information Security**: Threats, Vulnerabilities, Prevention, Detection, and Management. 6. dd. New Jersey: John Wiley & Sons. 10 mar 2006.

BLYTH, Michael.; **Business Continuity Management: Building an Effective Incident Management Plan**. United Stades: John Wiley & Songs, Inc, 2009

BON, Jan. **Fundamentos do gerenciamento de serviðos em TI: baseado no ITIL**.; Holanda. itSMF , 2006

BOTHA, J. **Managing E-Commerce in Business: Second Edition**. Cape Town, South Africa. Juta & company ltd. 2008.

CARALLI; Stevens; Young e Wilson. **Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.** Mai. 2007. Disponível em <http://www.cert.org/archive/pdf/07tr012.pdf> Acesso em: 08 OUT. 2012.

COELHO, Paulo. **Metodologias de análise de risco** Nov. 2005. Disponível em <http://ismspt.blogspot.com.br/2005/11/metodologias-de-anlise-de-risco.html> Acessado em 09. OUT.2012

DINSMORE, PAUL C. **AMA - Manual de Gerenciamento de Projetos**.; Rio de Janeiro. Brasport, 2009.

FLAMMINI, Francesco - **Critical Infrastructure Security: Assessment, Prevention, Detection, Response.** Ashurst Lodge - UK , Wit Press Ltda, 2012.

GARSON, David,. **Public Information Technology and E-Governance: Managing the Virtual State.**.; London, UK. Jones and Bartlett Inc. 2006.

GÓMEZ Ricardo; PÉREZ Diego; DONOSO, Yezid e HERRERA Andrea Abri. 2004 Disponível em <https://revistaing.uniandes.edu.co/pdf/A10%2031.pdf> Acesso em 15.OUT.2012

HOPKIN, Paul.; **Fundamentals of Risk Management: Understanding, Evaluating and Implementing effective risk management** - 2nd ed. Honk Kong. Graphicraft Ltda. 2010.

MANDARINI, Marcos.; **Segurança corporativa estratégica: fundamentos**. Barueri - São Paulo. Manole ltda. 2005;

MATTHYS, Eugeen.; **Business Continuity Management.** London: Benefolio Inc, 2009;

NBR/ISO 15999-1 e NBR/ISO 15999-2. Jun. 2011. Disponível em <http://www.slideshare.net/fdecicco/nbr-iso-31000-projeto-final-seg?from=embed> Acesso em: 23 SET. 2012.

NETO, Nelson Novaes. **Análise de Risco para Investimento de Segurança em Tecnologia da Informação**. 2005. Disponível em: http://www.psyzone.org/wp-content/uploads/2009/01/ra_nnnv3.pdf. Acesso em 07 nov 2012.

OCTAVE, Criteria. **Operationally critical threat, asset, and vulnerability evaluation**. (OCTAVE) Framework, Version 2.0. Disponível em http://www.cert.org/octave. Acesso em: 07 nov 2012.

OS&T Informática. **Pesquisa mostra que 83% das empresas devem aderir à virtualização nos próximos 12 meses** Jul. 2012. Disponível em <http://www.ost.com.br/novo/destaque.php?id=77> Acesso em: 15 SET. 2012.

PELTIER, T. **Information Security Risk Analysis,** 2nd ed. New York, NY: Auerbach Publications. Inc, 2005.

ABNT. **NBR ISO/IEC 17799 - Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação.** Rio de Janeiro, RJ: ABNT, 2005.

ABNT. **NBR ISO/IEC 31000 - Sistemas de gestão de qualidade - Princípios e diretrizes.** Rio de Janeiro, RJ: ABNT, 2009.

PONEMOM INSTITUTE. **Perceptions About Network Security**. Jun. 2011. Disponível em<http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf> Acesso em: 15 SET. 2012.

POTTS. John **Computer Security: A Bibliography With Indexes,** New York, NY Nova Scienc Publishers Inc, 2002.

PRESSMAN, Roger S.: **Engenharia de Software**. São Paulo: Makron Books Ltda. 2006.

RISKWORLD. Methodology. Disponível em http://www.riskworld.net/method.html Acesso em: 06/11/2012.

STROHL Brasil. **O que é GCN?** 2011. Disponível em <http://www.strohlbrasil.com.br/gcn.php> Acesso em: 10 OUT. 2012.

VAN GREUNING, Hennie. **Analyzing Banking Risk: A Framework for Assessing Corporate Governance and Risk Management.** 3 rd edition Washigton. DC: The World Bank Inc, 2009

ANEXOS

Nesta seção são apresentados os formulários que fazem parte da metodologia de avaliação de risco do OCTAVE.

ANEXOS A – Entrevista com a alta gerência

Levantamento do Gerenciamento Sênior				
Práticas	**Essa prática é usada por sua organização?**			
Conscientização de Segurança e Formação				
Os membros da equipe de segurança compreendem seus papéis e responsabilidades? Isso está documentado e verificado?	Sim	Não	**Parcial**	Não sei
Há experiência internamente adequada para todos os serviços suportados, mecanismos e tecnologias? (por exemplo, o registro, monitoramento, ou criptografia), incluindo a sua operação segura. Isto é documentado e verificado?	Sim	Não	**Parcial**	Não sei
Conscientização de segurança, treinamento e lembretes periódicos são fornecidas para toda a equipe? O não entendimento é documentado e conformidade é verificado periodicamente?	Sim	Não	**Parcial**	Não sei
Estratégia de Segurança				
As estratégias de negócio da organização rotineiramente incorpora considerações de segurança?	**Sim**	Não	Parcial	Não sei
Estratégias e políticas de segurança, leva em consideração as estratégias de negócio da organização e objetivos?	**Sim**	Não	Parcial	Não sei
Estratégias de segurança, metas e objetivos são documentadas e são revisados, atualizados, e comunicado à organização?	Sim	Não	**Parcial**	Não sei
Gestão de Segurança				
A gestão aloca fundos e recursos suficientes para as atividades de segurança da informação?	Sim	Não	**Parcial**	Não sei
As funções de segurança e responsabilidades são definidas para todos os funcionários da organização?	Sim	**Não**	Parcial	Não sei
As práticas de contratação e demissão de pessoas levam em conta questões de segurança da informação?	Sim	Não	**Parcial**	Não sei

Levantamento do Gerenciamento Sênior (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Gestão de Segurança (cont.)				
A organização gerencia os riscos de segurança da informação? Incluindo: • Avaliar os riscos à segurança da informação • Tomar medidas para mitigar os riscos de segurança da informação	Sim	Não	**Parcial**	Não sei
A gestão recebe e age de acordo com relatórios de rotina resumida relacionado à segurança de informação? (por exemplo, auditorias, registros de risco e avaliação de vulnerabilidade).	Sim	**Não**	Parcial	Não sei
Políticas de Segurança e Regulamentos				
A organização tem um conjunto abrangente de políticas atuais documentados, que são periodicamente revistos e actualizados?	Sim	**Não**	Parcial	Não sei
Existe um processo documentado para a gestão de políticas de segurança? Incluindo • Criação • Administração (incluindo revisões periódicas e atualizações) • Comunicação	Sim	**Não**	Parcial	Não sei
A organização tem um processo documentado para avaliar e garantir a conformidade com as políticas de segurança da informação, as leis e regulamentos aplicáveis, e seguro de requisites?	Sim	Não	**Parcial**	Não sei
A organização uniformemente reforça as políticas de segurança?	**Sim**	Não	Parcial	Não sei

Levantamento do Gerenciamento Sênior (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Gestão de Segurança Colaborativa				
A organização tem políticas e procedimentos para proteger a informação quando se trabalha com organizações externas? (por exemplo, os terceiros, colaboradores, subcontratados ou parceiros), incluindo: • Proteção de informações pertencentes a outras organizações • Compreender as políticas de segurança e procedimentos das organizações externas • A restrição de acesso a informações por entidades externas	**Sim**	Não	Parcial	Não sei
A organização verifica os serviços de segurança terceirizados, mecanismos e tecnologias de atender às suas necessidades e exigências?	Sim	Não	Parcial	**Não sei**
Planos de Contingência / Recuperação de Desastres				
Foi realizada uma análise da criticidade das operações, aplicações e dados?	**Sim**	Não	Parcial	Não sei
A organização tem documentado, revisado e testado? • A continuidade de negócios ou de emergência de planos da operação • O plano de recuperação de desastres • Plano de contingência para respostas a emergências	Sim	Não	**Parcial**	Não sei
Planos de continuidade de contingência, recuperação de desastres e de negócios considera os requisitos de acesso físico, eletrônico e controles?	Sim	Não	**Parcial**	Não sei
Todos os funcionários são: • Consciência da contingência, recuperação de desastres e planos de continuidade de negócios • Compreendem e são capazes de assumir as suas responsabilidades	Sim	Não	**Parcial**	Não sei

Levantamento do Gerenciamento Sênior (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Planos Físicas e Procedimentos de Segurança				
Planos de instalações e procedimentos de segurança para salvaguardar as instalações, os edifícios, e quaisquer áreas restritas são documentados e testados?	Sim	**Não**	Parcial	Não sei
Existem políticas e procedimentos documentados para o gerenciamento de visitantes?	Sim	Não	**Parcial**	Não sei
Existem políticas e procedimentos documentados para o controle físico de hardware e software?	Sim	Não	**Parcial**	Não sei
Controle de Acesso Físico				
Existem políticas e procedimentos documentados para controlar o acesso físico as áreas de trabalho, de hardware e de mídia de software? (por exemplo: computadores, dispositivos de comunicação, etc.)	Sim	Não	**Parcial**	Não sei
Estações de trabalho e outros componentes que permitem o acesso a informações sensíveis estão fisicamente protegidos para evitar o acesso não autorizado?	**Sim**	Não	Parcial	Não sei
Sistema e Gestão de Redes				
São documentados e testados planos de segurança para a salvaguarda dos sistemas e redes?	Sim	Não	**Parcial**	Não sei
Há um plano de backup de dados documentados e testados para backups de software e de dados? Todos os funcionários entendem suas responsabilidades no âmbito dos planos de backup?	Sim	Não	**Parcial**	Não sei
Autenticação e Autorização				
Existem políticas e procedimentos documentados para estabelecer e terminar o direito de acesso à informação para os indivíduos e grupos?	Sim	Não	**Parcial**	Não sei

Levantamento do Gerenciamento Sênior (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Gerenciamento de Incidentes				
Existem procedimentos documentados para identificar, relatar e responder a incidentes de segurança suspeitos e violados?	Sim	**Não**	Parcial	Não sei
Procedimentos de gestão de incidentes são periodicamente verificado, testado e atualizado?	Sim	**Não**	Parcial	Não sei
Existem políticas e procedimentos documentados para trabalhar com as agências de aplicação da lei?	Sim	Não	**Parcial**	Não sei
Práticas gerais do Pessoal				
Os membros da equipe segue boa prática de segurança? Tais como: • Informações para garantir que eles são responsáveis • Não divulgar informações confidenciais a outros • Ter capacidade adequada para utilizar o hardware de tecnologia da informação e software • Usando práticas de boas senhas • Compreender e seguir as políticas de segurança e regulamentos • Reconhecer e reportar incidentes	Sim	Não	**Parcial**	Não sei
Todos os funcionários em todos os níveis de responsabilidade implementam seus papéis e responsabilidades pela segurança da informação?	Sim	**Não**	Parcial	Não sei
Existem procedimentos documentados para autorizar e supervisionar todos os funcionários (incluindo pessoal de terceiros organizações) que trabalham com informações sensíveis ou que trabalham em locais onde a informação reside?	Sim	**Não**	Parcial	Não sei

Pesquisa Área de Gestão Operacional				
Práticas	**Essa prática é usada por sua organização?**			
Conscientização de Segurança e Formação				
Os membros da equipe de segurança entendem seus papéis e responsabilidades. Isso é documentado e verificado?	Sim	Não	**Parcial**	Não sei
Existem adequações internas e conhecimentos especializados para todos os mecanismos , tecnologias e serviços prestados? (por exemplo, o registro, monitoramento, ou criptografia), incluindo a sua operação segura. Isso é	Sim	Não	**Parcial**	Não sei
Conscientização de segurança, treinamento e lembretes periódicos são fornecidos para todo o pessoal? O entendimento da equipe é documentado e conformidade é verificado periodicamente?	Sim	Não	**Parcial**	Não sei
Estratégia de Segurança				
As estratégias de negócio da organização rotineiramente incorporam considerações de segurança?	**Sim**	Não	Parcial	Não sei
As estratégias e políticas de segurança levam em consideração as estratégias de negócio da organização **e** seus objetivos?	**Sim**	Não	Parcial	Não sei
Estratégias de segurança, metas e objetivos são documentadas e revisados, atualizados e comunicados periodicamente à organização?	Sim	Não	**Parcial**	Não sei
Gestão de Segurança				
A gestão aloca fundos e recursos suficientes para as atividades de segurança da informação?	Sim	Não	**Parcial**	Não sei
As funções de segurança e responsabilidades são definidas para todos os funcionários da organização?	Sim	**Não**	Parcial	Não sei
As práticas de contratação e demissão de pessoas levam em conta questões de segurança da informação?	Sim	Não	**Parcial**	Não sei

Pesquisa Área de Gestão Operacional (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Gerenciamento de Segurança				
A organização gerencia os riscos de segurança da informação? Incluindo: • Avaliar os riscos à segurança da informação • Tomar medidas para mitigar os riscos de segurança da informação	Sim	Não	**Parcial**	Não sei
A gestão recebe e age de acordo com relatórios de rotina resumindo informações relacionadas à segurança? (por exemplo, auditorias, registros de risco e avaliação de vulnerabilidade).	Sim	**Não**	Parcial	Não sei
Políticas de Segurança e				
A organização tem um conjunto abrangente de políticas atuais documentados, que são periodicamente revisados e atualizados?	Sim	**Não**	Parcial	Não sei
Existe um processo documentado para a gestão de políticas de segurança? Incluindo: • criação • Administração (incluindo revisões periódicas e atualizações) • Comunicação	Sim	**Não**	Parcial	Não sei
A organização tem um processo documentado para avaliar e garantir a conformidade com as políticas de segurança da informação, as leis e regulamentos aplicáveis e requisitos de seguros?	Sim	Não	**Parcial**	Não sei
A organização uniformemente reforça as políticas de segurança?	**Sim**	Não	Parcial	Não sei

Pesquisa Gestão Operacional Área (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Gestão de Segurança Colaborativa				
A organização tem políticas e procedimentos para proteger as informações quando se trabalha com organizações externas? (por exemplo, terceiros, colaboradores, subcontratados, ou parceiros), incluindo: • Proteção de informações pertencentes a outras organizações • Compreensão das políticas de segurança e procedimentos das organizações externas • O acesso à informação por fim terminadas pessoal externo	**Sim**	Não	Parcial	Não sei
A organização verificou que os serviços de segurança, mecanismos e tecnologias de empresas terceirizadas para atender às suas necessidades e	Sim	Não	Parcial	**Não sei**
Planos de Contingência / Recuperação de Desastres				
Foi realizada uma análise das criticidades das operações, aplicações e de dados?	Sim	**Não**	Parcial	Não sei
A organização tem documentado, revisado e testado? • Continuidade de negócios ou de emergência planos de operação • O plano de recuperação de desastres (s) • Plano de contingência (s) para resposta a emergências	Sim	Não	**Parcial**	Não sei
Os planos de contingência, recuperação de desastres e de continuidade de negócios consideram os requisitos de acesso físico e eletrônico e controles?	Sim	Não	**Parcial**	Não sei
Todos os funcionários são: • Conhecimento da contingência, recuperação de desastres e planos de continuidade de negócios • Compreender e a capacidade de assumir as suas responsabilidades	Sim	**Não**	Parcial	Não sei

Pesquisa na área de gestão operacional (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Planos de segurança física e procedimentos				
Planos de instalações e procedimentos de segurança para salvaguardar as instalações, os edifícios, e quaisquer áreas restritas são documentados e	Sim	**Não**	Parcial	Não sei
Existem políticas e procedimentos documentados para o gerenciamento de visitantes?	Sim	Não	**Parcial**	Não sei
Existem políticas e procedimentos documentados para o controle físico de hardware e software?	Sim	Não	**Parcial**	Não sei
Controle de Acesso Físico				
Existem políticas e procedimentos documentados para controlar o acesso físico a áreas de trabalho de hardware e de mídia de software? (por exemplo: computadores, dispositivos de comunicação, etc.)	Sim	Não	**Parcial**	Não sei
Estações de trabalho e outros componentes que permitem o acesso a informações confidenciais estão fisicamente protegidos para evitar o acesso não	**Sim**	Não	Parcial	Não sei
Monitoramento e Auditoria de Segurança Física				
Registros de auditoria e monitoramento são examinadas rotineiramente para as anomalias, e são tomadas medidas corretivas quando necessário?	Sim	**Não**	Parcial	Não sei
Sistema e Gestão de Redes				
São documentados e testados os plano de segurança para a salvaguarda dos sistemas e redes?	Sim	Não	**Parcial**	Não sei
Há um plano de backup de dados documentados e testados para backups de software e dados? Todos os funcionários entendam suas responsabilidades no âmbito dos planos de backup?	Sim	Não	**Parcial**	Não sei
Autenticação e Autorização				
Existem políticas e procedimentos documentados para estabelecer e terminar o direito de acesso à informação para indivíduos e grupos?	Sim	Não	**Parcial**	Não sei

Pesquisa na área de gestão operacional (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Gerenciamento de Incidentes				
Existem procedimentos documentados para identificar, relatar e responder a incidentes de segurança suspeitos e violações?	Sim	**Não**	Parcial	Não sei
Procedimentos de gestão de incidentes são periodicamente testados, verificados e atualizados?	Sim	**Não**	Parcial	Não sei
Existem políticas e procedimentos documentados para trabalhar com órgãos na aplicação da lei?	Sim	Não	**Parcial**	Não sei
Práticas Gerais da Equipe				
Os membros da equipe seguem boas práticas de segurança? Tais como: • Informações para garantir que eles são responsáveis • Não divulgar informações confidenciais a outros (resistência à engenharia social) • Ter capacidade adequada para utilizar o hardware de tecnologia da informação e software • Utilizando boas senhas • Compreender e seguir as políticas de segurança e regulamentos	Sim	Não	**Parcial**	Não sei
Todos os funcionários em todos os níveis de responsabilidade usam seus papéis e responsabilidades pela segurança da informação?	Sim	**Não**	Parcial	Não sei
Existem procedimentos documentados para autorizar e supervisionar todos os funcionários (incluindo por pessoal competente de terceiros organizações) que trabalham com informações sensíveis ou que trabalham em locais onde a informação reside?	Sim	**Não**	Parcial	Não sei

Levantamento da Equipe				
Práticas	**Essa prática é usada por sua organização?**			
Conscientização de Segurança e Formação				
Os membros da equipe de segurança entendem seus papéis e responsabilidades? Isso é documentado e verificado?	Sim	Não	**Parcial**	Não sei
Há adequações internas e especialização para todos os serviços, mecanismos e tecnologias suportados? (por exemplo, o registro, monitoramento, ou criptografia), incluindo a sua operação segura. Isso é documentado e verificado?	Sim	Não	**Parcial**	Não sei
Conscientização de segurança, treinamento e lembretes periódicos são fornecidos para todo o pessoal? O entendimento da equipe é documentado e conformidade é verificado periodicamente?	Sim	Não	**Parcial**	Não sei
Gestão de Segurança				
A gestão para atribuir fundos e recursos suficientes para as atividades de segurança da informação?	Sim	**Não**	Parcial	Não sei
As funções de segurança e responsabilidades são definidas para todos os funcionários da organização?	Sim	**Não**	Parcial	Não sei
Contratação da organização e a rescisão do pessoal levam a as questões de segurança da informação em conta?	Sim	Não	**Parcial**	Não sei
A organização gerencia os riscos de segurança da informação? Incluindo: • Avaliar os riscos à segurança da informação • Tomar medidas para mitigar os riscos de segurança da informação	Sim	Não	**Parcial**	Não sei

Levantamento da Equipe (cont.)					
Práticas	**Essa prática é usada por sua organização?**				
Políticas de Segurança e Regulamentos					
A organização tem um conjunto abrangente de políticas atuais documentadas e que são periodicamente revisados e atualizados?	**7**	Sim	**Não**	Parcial	Não sei
Existe um processo documentado para a gestão de políticas de segurança? Incluindo: • Criação • Administração (incluindo revisões periódicas e atualizações)		Sim	**Não**	Parcial	Não sei
A organização uniformemente reforça as políticas de segurança?		Sim	Não	**Parcial**	Não sei
Gestão de Segurança Colaborativa					
A organização tem políticas e procedimentos para proteger as informações quando se trabalha com organizações externas? (por exemplo, terceiros, colaboradores, subcontratados, ou parceiros), incluindo: • Proteção de informações pertencentes a outras organizações • Compreensão das políticas de segurança e procedimentos das organizações externas • O acesso à informação por fim terminadas pessoal externo		**Sim**	Não	Parcial	Não sei
Planos de Contingência / Recuperação de Desastres					
Todos os funcionários estão: • Conscientes da contingência, recuperação de desastres e planos continuidade de negócios. • Entendem a capacidade de assumir as suas responsabilidades		Sim	**Não**	Parcial	Não sei
Planos Físicos e Procedimentos de Segurança					

Planos de instalações e procedimentos de segurança para salvaguardar as instalações, os edifícios, e áreas restritas são documentados testados?	Sim	**Não**	Parcial	Não sei

Levantamento da Equipe (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Existem políticas e procedimentos documentados para gerenciar visitantes?	Sim	Não	**Parcial**	Não sei
Existem políticas e procedimentos documentados para o controle físico de hardware e software?	Sim	Não	**Parcial**	Não sei
Controle de Acesso Físico				
Existem políticas e procedimentos documentados para controlar o acesso físico a áreas de trabalho de hardware e de mídia de software? (computadores, dispositivos de comunicação, etc.)	Sim	Não	**Parcial**	Não sei
Estações de trabalho e outros componentes que permitem o acesso a informações sensíveis estão fisicamente protegidos para evitar o acesso não	**Sim**	Não	Parcial	Não sei
Sistema e Gestão de Redes				
Há um plano de backup dos dados documentado e testado para backups de software e dados. Todos os funcionários entendam suas responsabilidades no âmbito dos planos de backup?	Sim	Não	**Parcial**	Não sei
Gerenciamento de incidentes				
Existem procedimentos documentados para identificar, relatar e responder a incidentes de segurança suspeitos e violações?	Sim	**Não**	Parcial	Não sei
Procedimentos de gestão de incidentes são periodicamente testados, verificados e atualizados?	Sim	**Não**	Parcial	Não sei
Existem políticas e procedimentos documentados para trabalhar com as agências de aplicação da lei?	Sim	Não	**Parcial**	Não sei

Levantamento da Equipe (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Práticas gerais dos Funcionários				
Os membros da equipe seguem boas práticas de segurança? Tais como: • Segurança da informação para as quais eles são responsáveis • Não divulgar informações confidenciais a outros (resistência à engenharia social) • Ter capacidade adequada para utilizar o hardware de tecnologia da informação e software • Usado senhas seguras	Sim	Não	**Parcial**	Não sei
Todos os funcionários em todos os níveis de responsabilidade implementam seus papéis e responsabilidades pela segurança da informação?	Sim	**Não**	Parcial	Não sei
Existem procedimentos documentados para autorizar e supervisionar todos os funcionários (incluindo por pessoal competente de terceiros organizações) que trabalham com informações sigilosas ou que trabalham em locais onde a informação reside?	Sim	**Não**	Parcial	Não sei

Levantamento de Equipe de TI				
Práticas	**Essa prática é usada por sua organização?**			
Conscientização de Segurança e				
Os membros da equipe de segurança compreender seus papéis e responsabilidades? Isso está documentado e verificado?	Sim	Não	**Parcial**	Não sei
Não é adequada internamente conhecimentos especializados para todos os serviços suportados, mecanismos e tecnologias? (por exemplo, registro, monitoramento, ou criptografia), incluindo a sua operação segura. Isso está documentado e verificado?	Sim	Não	**Parcial**	Não sei
Conscientização de segurança, treinamento e lembretes periódicos são fornecidos para todo o pessoal? Pessoal sob a compreensão é documentado e conformidade é verificado periodicamente?	Sim	Não	**Parcial**	Não sei
Estratégia de Segurança				
Estratégias de negócio da organização habitualmente incorporam considerações de segurança?	**Sim**	Não	Parcial	Não sei
Estratégias e políticas de segurança leva em consideração as estratégias de negócio da organização e objetivos?	**Sim**	Não	Parcial	Não sei
Estratégias de segurança, metas e objetivos são documentadas e são revisados, atualizados e comunicada à organização?	Sim	Não	**Parcial**	Não sei
Gestão de Segurança				
A gestão aloca fundos e recursos suficientes para as atividades de segurança da informação?	Sim	**Não**	Parcial	Não sei
Direitos de acesso e responsabilidades são definidas para todos os funcionários da organização?	**Sim**	Não	Parcial	Não sei

Levantamento de Equipe de TI (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Gestão de Segurança (cont.)				
Contratações pela organização e práticas de rescisão do pessoal levam as questões de segurança da informação em conta?	Sim	Não	Parcial	Não sei
A organização gerencia os riscos de segurança da informação? Incluindo: • Avaliar os riscos à segurança da informação • Tomar medidas para mitigar os riscos de segurança da informação	Sim	Não	**Parcial**	Não sei
Gestão recebe e age de acordo com relatórios de rotina resumindo informações de segurança? (por exemplo, auditorias, registros de risco e avaliação de vulnerabilidade).	Sim	**Não**	Parcial	Não sei
Políticas de Segurança e Regulamentos				
A organização tem um conjunto abrangente de políticas atuais documentados, que são periodicamente revisados e atualizados?	Sim	Não	**Parcial**	Não sei
Existe um processo documentado para a gestão de políticas de segurança? Incluindo: • Administração (incluindo revisões periódicas e atualizações) • Comunicação • Criação	Sim	**Não**	Parcial	Não sei
A organização tem um processo documentado para avaliar e garantir a conformidade com as políticas de segurança de informações, leis e regulamentos aplicáveis e requisitos de seguros?	Sim	Não	**Parcial**	Não sei
A organização uniformemente reforça as políticas de segurança?	**Sim**	Não	Parcial	Não sei

Levantamento de Equipe de TI (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Gestão de Segurança				
A organização tem políticas e procedimentos para proteger a informação quando se trabalha com organizações externas (por exemplo, terceiros, colaboradores, subcontratados, ou parceiros), incluindo: • proteção de informações pertencentes a outras organizações • compreender as políticas de segurança e procedimentos das organizações externas • O acesso à informação por fim terminadas pessoal externo	**Sim**	Não	Parcial	Não sei
A organização verificou que os serviços de segurança terceirizados, mecanismos e tecnologias para atender às suas necessidades e exigências.	Sim	Não	Parcial	**Não sei**
Planos de Contingência / Recuperação de Desastres				
Foi realizada uma análise das criticidades das operações, aplicações e de dados?	**Sim**	Não	Parcial	Não sei
A organização tem documentado, revisado e testado? • Continuidade de negócios ou de emergência planos de operação • O plano de recuperação de desastre (s) • Plano de contingência (s) para resposta a emergências	Sim	Não	**Parcial**	Não sei
Planos de continuidade de contingência, recuperação de desastres de negócios consideram ósmio requisitos de acesso físico de controles eletrônico?	Sim	Não	**Parcial**	Não sei
Todos os funcionários possui: • Consciência da contingência, recuperação de desastres e planos de continuidade de negócios	Sim	Não	**Parcial**	Não sei

Levantamento de Equipe de TI (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Segurança Física e planos de procedimento				
Planos de instalações e procedimentos de segurança de proteção das instalações, dos edifícios, e quaisquer áreas restritas são documentados e testados?	Sim	**Não**	Parcial	Não sei
Existem políticas e procedimentos documentados para o gerenciamento de visitantes?	Sim	Não	**Parcial**	Não sei
Existem políticas e procedimentos documentados para o controle físico de hardware e software?	Sim	Não	**Parcial**	Não sei
Controle de Acesso Físico				
Existem políticas e procedimentos documentados para controlar o acesso físico a áreas de trabalho de hardware e de mídia de software? (por exemplo, computadores, dispositivos de comunicação, etc.)	Sim	Não	**Parcial**	Não sei
Estações de trabalho e outros componentes que permitem o acesso a informações sigilosas estão fisicamente protegidos para evitar o acesso não autorizado?	**Sim**	Não	Parcial	Não sei
Monitoramento e Auditoria de Segurança				
Registros de manutenção são mantidos para documentar os reparos e modificações de componentes físicos de uma unidade de saúde?	Sim	**Não**	Parcial	Não sei
As ações de um indivíduo ou grupo, com respeito a todos os meios físicos controlados, podem ser contabilizados?	Sim	Não	**Parcial**	Não sei
Registros de auditoria e monitoramento são examinadas rotineiramente para as anomalias, e são tomadas medidas corretas quando necessário?	Sim	Não	**Parcial**	Não sei
Sistema e Gestão de Redes				
Existe documentações e plano de segurança (s) testados para a salvaguarda dos sistemas e redes?	Sim	Não	**Parcial**	Não sei

Levantamento de Equipe de TI (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Informações sigilosas são protegidas por armazenamento seguro? (por exemplo, backups armazenados fora do local, processo para descartar informações sensíveis).	Sim	Não	**Parcial**	Não sei
A integridade do software instalado é regularmente verificada?	Sim	**Não**	Parcial	Não sei
Todos os sistemas estão atualizados e com respeito a revisões, correções e recomendações em alertas de segurança?	Sim	Não	**Parcial**	Não sei
Há um plano de backup de dados documentados e testados para backups de software e dados. Todos os funcionários entendam suas responsabilidades no âmbito dos	Sim	Não	**Parcial**	Não sei
Alterações de hardware e software são planejadas, controladas e documentadas?	Sim	Não	**Parcial**	Não sei
Membros da equipe de TI seguem os procedimentos quando da emissão, alteração e encerramento senhas de usuários, contas e privilégios? • Identificação do usuário único é exigido para todos os usuários do sistema de informação, incluindo usuários de terceiros. • As contas e senhas padrão foram removidas do sistema.	Sim	Não	**Parcial**	Não sei
Apenas os serviços necessários estão em execução em sistemas - todos os serviços desnecessários foram removidos?	**Sim**	Não	Parcial	Não sei
Ferramentas de Administração do Sistema				
Ferramentas e mecanismos para o sistema de seguro e administração de rede são usados, e são revisados e atualizados ou substituídos?	Sim	Não	Parcial	**Não sei**

Levantamento de Equipe de TI (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Monitoramento e auditoria de segurança de TI				
Sistema e rede de monitoramento e ferramentas de auditoria são rotineiramente utilizados pela organização? Atividade incomum é tratada de acordo com a política apropriada ou procedimento?	**Sim**	Não	Parcial	Não sei
Componentes de segurança de firewall e outros são periodicamente auditados para o cumprimento da política?	Sim	Não	**Parcial**	Não sei
Autenticação e Autorização				
Controles de acesso apropriados e autenticação de usuário (por exemplo, permissões de arquivos, configuração de rede) consistente com a política são usados para restringir o acesso do usuário à informação, sistemas críticos, aplicações e serviços	Sim	Não	**Parcial**	Não sei
Existem políticas e procedimentos documentados para estabelecer e terminar o direito de acesso à informação para indivíduos e grupos?	Sim	Não	**Parcial**	Não sei
Métodos ou mecanismos são fornecidos para garantir que informações confidenciais não foram acessadas, alterados ou destruídos de forma não autorizada? Métodos ou mecanismos são periodicamente revisados e verificados?	Sim	**Não**	Parcial	Não sei

Levantamento de Equipe de TI (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Gerenciamento de Vulnerabilidades				
Há um conjunto de procedimentos documentados para vulnerabilidades de gestão? Incluindo: • Seleção de ferramentas de avaliação de vulnerabilidade, listas de verificação e scripts • Manter-se atualizado com os tipos de vulnerabilidades conhecidas e métodos de ataque • Revisão das fontes de informações sobre os anúncios de vulnerabilidade, alertas de segurança e avisos • Identificar os componentes de infraestrutura a serem avaliados	Sim	**Não**	Parcial	Não sei
Procedimentos de gerenciamento de vulnerabilidades são seguidas e são periodicamente revisados e atualizados?	Sim	Não	**Parcial**	Não sei
Avaliações de vulnerabilidade de tecnologia são realizadas em uma base periódica, e as vulnerabilidades são abordados quando eles são identificados?	Sim	**Não**	Parcial	Não sei
Criptografia				
Controles de segurança apropriados são usados para proteger informações sensíveis durante o armazenamento e durante a transmissão? (por exemplo, criptografia de dados, infraestrutura de chave pública, tecnologia de rede privada virtual).	**Sim**	Não	Parcial	Não sei
Protocolos criptografados são utilizados quando o gerenciamento remoto de sistemas, roteadores e firewalls?	**Sim**	Não	Parcial	Não sei

Levantamento de Equipe de TI (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Arquitetura de Segurança e Design				
Arquitetura do sistema e projeto para sistemas novos e revisados incluem considerações sobre: • Estratégias de segurança, políticas e procedimentos • História de comprometimento da segurança • Resultados das avaliações de riscos de segurança	**Sim**	Não	Parcial	Não sei
Existem procedimentos documentados para autorizar e supervisionar todos os funcionários (incluindo pessoal de terceiros organizações) que trabalham com informações sensíveis ou que trabalham em locais onde a informação reside?	Sim	**Não**	Parcial	Não sei
Gerenciamento de incidentes				
Existem procedimentos documentados para identificar, relatar e responder a suspeitas de segurança incidentes e violações?	Sim	**Não**	Parcial	Não sei
Procedimentos de gestão de incidentes são periodicamente testado, verificado e atualizados?	Sim	**Não**	Parcial	Não sei
Existem políticas e procedimentos documentados para trabalhar com as agências de aplicação da lei?	Sim	Não	**Parcial**	Não sei

Levantamento de Equipe de TI (cont.)				
Práticas	**Essa prática é usada por sua organização?**			
Práticas gerais do pessoal				
Os membros da equipe seguem boas práticas de segurança? Tais como: • Informações para garantir que eles são responsáveis • Não divulgar informações confidenciais a outros (resistência à engenharia social) • Ter capacidade adequada para utilizar o hardware de tecnologia da informação e software • Usar boas senhas • Compreender e seguir as políticas de segurança e regulamentos • Reconhecer e reportar incidentes	Sim	Não	**Parcial**	Não sei
Todos os funcionários em todos os níveis de responsabilidade implementam seus papéis e responsabilidades pela segurança da informação?	Sim	**Não**	Parcial	Não sei
Existem procedimentos documentados para autorizar e supervisionar todos os funcionários (incluindo pessoal de terceiros organizações) que trabalham com informações sensíveis ou que trabalham em locais onde a informação reside?	Sim	**Não**	Parcial	Não sei

88