UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

FABRÍCIO DE JESUS DE LIMA

ESTUDO DE MELHORIAS EM SEGURANÇA DE INFORMAÇÃO

MONOGRAFIA

CURITIBA
2013

FABRÍCIO DE JESUS DE LIMA

ESTUDO DE MELHORIAS EM SEGURANÇA DA INFORMAÇÃO

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Programa de Pós-Graduação em Tecnologia. Universidade Tecnológica Federal do Paraná. Área de Concentração: Redes de Computadores
Orientador: Prof. MSc. Luis Rohling

CURITIBA
2013

RESUMO

LIMA, Fabrício J. **Estudo de melhorias em segurança da informação.** 2013. 66 f.Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

A presente monografia aborda o estudo para a implementação de técnicas de melhorias em segurança da informação, buscando auxiliar na compreensão e tratamento dos riscos, visando saná-los, diminuir seu impacto ou aceitá-lo caso ainda não seja oportuno ou prioritário. O projeto inicializa-se utilizando método bibliográfico, seguido de estudo em campo, inventário, escolha e tratamento do incidente.

Palavras-chave: Gestão de Riscos. ISO 27000. Segurança da Informação. Auditoria de Redes. Governança de TI. ITIL. COBIT. Gerenciamento de TI.

ABSTRACT

MEGGER, Chrystian L. **Study improvements in information security.** 2011. 66.pages. Monograph (Specialization in Configuration and Management of Servers and Network Equipments). Federal Technological University of Paraná. Curitiba, 2013.

This monograph discusses the study for the implementation of technical improvements in information security, seeking help in understanding and treating risks, aiming address them, lessen their impact or accept it if it is not timely or priority. The project starts up using bibliographical method, followed by field study, inventory, choice and treatment of the incident.

Keywords: Risk Management. ISO 27000. Information Security. Audit Networks. IT Governance. ITIL. COBIT. IT Management.

LISTA DE SIGLAS

ABNT - Associação Brasileira de Normas Técnicas
AS/NZS - Austrália e Nova Zelândia
BSI - *British Standart International*
CFTV - Circuito Fechado de Televisão
CMMI - *Capability Maturity Model Integration*
COBIT - *Control Objectives for Information and Related Technology*
COSO - *Committee of Sponsoring Organizations of the Treadway Commission*
CPD - Centro de Processamento de Dados
IBCA - Instituto Brasileiro de Conselheiros de Administração
IBGC - Instituto Brasileiro de Governança Corporativa
IDS - *Intrusion Detection System*
IEC - *International Electrotechnical Commission*
IPS - *Intrusion Prevention System*
IPSEC - *Internet Protocol Security*
ISACA - Associação de Auditoria e Controle de Sistemas de Informação
ISO - *International Organization for Standardization*
ITIL - *Information Technology Infrastructure Library*
LAN - *Local Area Network*
LP - *Louisiana Pacific*
MARAT - Método de Análise de Riscos e Acidentes de Trabalho
MDF - *Medium-Density Fiberboard*
MDP - *Medium Density Paticleboard*
NBR – Norma Brasileira
OSB - *Oriented Strand Board*
PABX - *Private Branch Exchange*
PDCA - *Plan-Do-Check-Act*
PMBOK - *Project Management Body of Knowledge*
RAID - *Redundant Array Of Independent Disks*
SAP - *Systems, Applications, and Products in Data Processing*
SGSI - *Sistema de Gestão de Segurança da Informação*
SOX - *Sarbane-Oxley*
VLAN – *Virtual Local Area Network*
VPN - *Virtual Private Network*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo serão tratados os elementos introdutórios relacionados ao estudo implementação de técnicas de melhorias em segurança da informação.

1.1 TEMA

Tendo em vista Nem toda informação é vital, porém determinadas informações podem ser tão importantes e necessárias que qualquer custo aplicado para manter sua integridade seria nada se comparado ao custo de não dispor de tais informações.

O ambiente de negócios exige cada vez mais que a informação seja acessível de qualquer parte do mundo, por meio de pontos remotos e tecnologias móveis, com a mesma segurança, integridade e velocidade que o suportado dentro das *intranets* das organizações. Tendo em vista tal demanda, é de fundamental importância e como quesito de sobrevivência, que se tenha um conjunto de controles, como políticas, processos e procedimentos. Devendo ser constantemente revisados, corretamente aplicados e monitorados, a fim do seu real cumprimento.

Neste trabalho, será abordada as principais técnicas que padronizam a forma como as organizações enxergam e protegem sua informação, tratando dos riscos com o foco no negócio.

1.2 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

1.2.1 Objetivo Geral

O principal objetivo deste projeto é direcionar a organização na busca da melhor proteção para a informação bem como maior eficiência e eficácia no tratamento dos riscos inerentes.

1.2.2 Objetivos Específicos

- Identificar a necessidade de proteção da informação
- Identificar os métodos mais utilizados para a padronização da segurança da informação
- Levantar cenário da empresa avaliada
- Estudo das principais ameaças
- Avaliação da aceitabilidade do risco
- Elaboração da proposta de implementação de melhoria da segurança

1.3 JUSTIFICATIVA

Grande parte das empresas, mesmo sendo de grande porte ou elevado faturamento anual, ainda não identifica a necessidade de se reestruturar a área de Tecnologia da Informação, visando a proteção da informação além da ação reativa dos incidentes que surgem como que por “combustão espontânea”. Este estudo apresentará os recursos mais utilizados pelas empresas de sucesso que vem se tornando um diferencial ou exigência na maioria dos tratados e fechamentos de acordos de negócio.

1.4 PROCEDIMENTOS METODOLÓGICOS

Seguindo a linha de raciocínio de Fontes (2011) sobre o processo de segurança da informação, levando em consideração os objetivos das principais normas das famílias ISO/IEC 27000 e ISO/IEC 31000. O estudo feito por Coelho *et. al.* (2010), enfatiza a area governança de tecnlogia como braço

direito da gorvernança corporativa. Em seguida, é apresentado o método COBIT e seu modelo de maturidade. O ITIL é encaixado no processo de Desenho de Serviços, titulado como função de Gerenciamento de Segurança de Informação. Este trabalho de monografia estará seguindo os procedimentos técnicos de pesquisa bibliográfica e estudo de campo.Já o estudo de campo é definido com base na gestão de riscos da ISO/IEC 27005. A análise forense é feita através no estudo de Método de Análise de Riscos e Acidentes de Trabalho – MARAT, permite hierarquizar de modo racional a prioridade de eliminação, minimização e/ou controle do risco.

2 REFERENCIAIS TEÓRICOS

2.1 VALOR DA INFORMAÇÃO PARA AS ORGANIZAÇÕES

A informação é o elemento fundamental para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor, podendo levar a organização do sucesso ao fracasso, em função de impactos financeiros, operacionais ou de imagem, ocasionados por falhas, erros ou fraudes no uso da informação. “O que diferencia o uso da informação entre as organizações é a necessidade de se manter disponível, mantendo a integridade e o rigor em relação ao sigilo que cada organização precisa para a sua informação" (FONTES, 2011, p. 2).

A informação, a partir desse ponto, passa a ser um recurso estratégico para qualquer organização, de forma a gerar conhecimento e através dos recursos de tecnologia, podendo ser compartilhado, a fim de agregar valor na rápida tomada das decisões do negócio. Com isso, se maximiza os benefícios e o retorno dos investimentos, capitalizando as oportunidades e ganhando em poder competitivo.

(WADLOW, 2000 *apud* MATOS, 2010) classifica a informação em níveis de prioridade, enfatizando a importância da classe de informação, respeitando as necessidades da empresa:

- **Pública**: Informação que pode vir a público sem maiores conseqüências danosas ao funcionamento normal da empresa, e cuja integridade não é vital.
- **Interna**: O acesso livre a este tipo de informação deve ser evitado, embora as conseqüências do uso não autorizado não sejam sérias. Sua integridade é importante, mesmo que não seja vital.
- **Confidencial**: Informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo.
- **Secreta**: Informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número reduzido de pessoas. A segurança desse tipo de informação é vital para a companhia.

Segundo Fontes (2011), a informação, sendo um ativo intangível de significativa importância para qualquer organização, independentemente do seu porte e do seu segmento de mercado, deve irrevogavelmente ser

considerada a necessidade de se ter uma proteção adequada por meio dos processos de Segurança da Informação.

Segundo Lima (2010), independentemente do meio ou forma pela qual a informação é manuseada, armazenada, transmitida, e descartada, é recomendável que ela passe por processos de proteção e controles adequados a cada meio e/ou forma de tratamento.

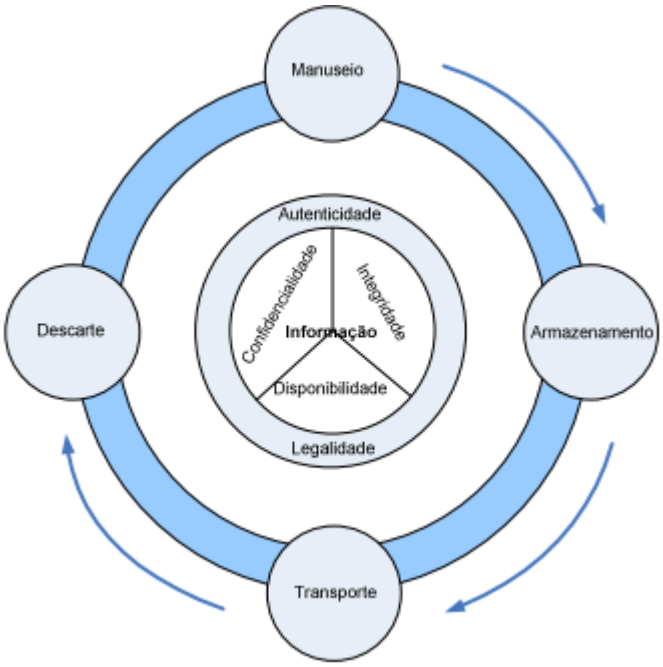


Figura 1: Ciclo de Vida da Informação
Fonte: (SÊMOLA 2003, p. 11 *apud* SILVEIRA 2009)

2.2 A SEGURANÇA DA INFORMAÇÃO

Fontes (2011) afirma que “O processo de segurança da informação existe para possibilitar que a organização utilize de maneira confiável os recursos que suportam as informações necessárias para as suas atividades estratégicas, táticas e operacionais.”

A segurança da informação deve existir para proteger os recursos de informação que são utilizados estratégica e operacionalmente para o funcionamento da organização, contra divulgação indevida, seja ela intencional ou não, alteração não autorizada, destruição não desejada, negação de serviço, fraudes financeiras, apropriação indevida de informações ou reputação da imagem da instituição. Essa proteção é feita através da implantação de controles de segurança definidos em políticas e procedimentos. Porém, Fontes (2011) destaca que “[...]nenhuma política deve ser criada para atender a própria segurança somente para estar em conformidade com os requerimentos

de auditoria, mas para proteger os recursos de informação e seus objetivos de negócio de forma a assistir de acordo com necessidade da organização.”

A segurança da informação é classificada em três princípios básicos: (PEIXOTO, 2006 *apud* ALVES, 2010)

- Integridade: É a garantia de que as informações não sofreram nenhuma modificação não autorizada da sua origem ao seu destino, garantindo assim a sua real veracidade.

- Confidencialidade: Princípio que trata sobre a disponibilidade de informações à apenas pessoas autorizadas. Várias tecnologias como, por exemplo, criptografia e autenticações podem ser usadas, desde que mantenham a integridade das informações.

- Disponibilidade: De nada adianta possuir integridade e confidencialidade, se a informação nunca está disponível. *Nobreaks*, *RAID*, Sistemas Redundantes, *backups* são alguns dos agentes responsáveis por é manter essa estrutura de passagem de informações de forma confiável e integra sem que haja impossibilidade de consultar e alimentar as informações.

Outros critérios de controle se fazem relevantes em alguns modelos de gestão de segurança da informação:

- Efetividade: a informação sendo entregue em tempo, de maneira correta, consistente e utilizável.

- Eficiência: entrega da informação através do mais produtivo e econômico uso dos recursos.

- Conformidade ou Legalidade: de acordo com as leis, regulamentos, políticas internas e obrigações contratuais impostos externamente.

- Confiabilidade: entrega da informação apropriada para os executivos para administrar a entidade e exercer suas responsabilidades fiduciárias e de governança.

- Autenticidade e Não Repúdio: tem como objetivo verificar a identidade e autenticidade de alguém ou até mesmo de um agente exterior a fim de garantir a integridade de origem.

Alves (2010) afirma que os controles acima envolvem três aspectos principais:

- Pessoas: Usuários treinados e conscientizados.

- Processos: Políticas claras para utilização dos recursos tecnológicos fornecidos pela empresa.

- Tecnologia: Sistemas monitorados e seguros para garantir a proteção da informação.

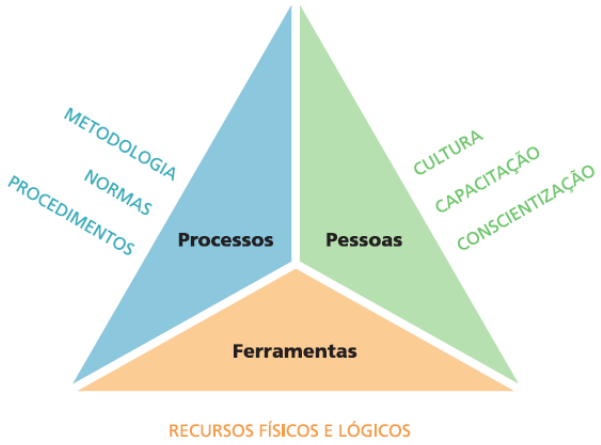


Figura 2: Gestão de Segurança da Informação
Fonte: Promon (2005)

2.1.1 A Importância da Política de Segurança da Informação

As políticas de Segurança de Informação são responsáveis pela estruturação das melhores práticas para a elaboração, implantação e eficacidade dos processos de segurança, bem como as definições das diretrizes, limitando e direcionando os objetivos da organização.

A política é o mais alto nível de declaração do que a organização acredita e quer que exista em todas as suas áreas. A política é uma diretiva da direção executiva para criar um programa de segurança da informação, estabelecer seus objetivos e definir responsabilidades; As regras definidas valem para todos. E se o tratamento for diferente para tipos de usuários diferentes, esta definição deve estar formalizada na política e nos demais regulamentos de segurança da informação (Fontes, p.15. 2011). Por elas mesmas, não definem sua maneira de aplicação, mas apenas orientações básicas que auxiliam no enquadramento dos controles ao tipo de necessidade do negócio. Já as normas, ditam as regras iniciais da implementação do controle, que por sua vez, é detalhado em forma de procedimentos.

> *A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware*
>
> *Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário,*

para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. (ABNT, 2005, p.x)

Esses regulamentos são chamados Procedimentos de Segurança de Informação (PSI), são específicos para cada organização, com base nas melhores práticas, por ela adotadas. E seu grau de complexidade está diretamente proporcional ao valor da informação. Para a criação de uma PSI, devemos primeiramente levar em consideração o motivo que levou a ter essa política. Seja ele legislativo ou tendências de mercado, focado na proteção mais adequada, com base no *custo x benefício*. A participação do Financeiro, dos Recursos Humanos e Gestores são imprescindíveis na criação de qualquer política. Departamentos como o Jurídico, também tem um papel fundamental em algumas aplicações de políticas, para que se cumpra a legislação em vigor.

Fontes (2011) classifica os conjuntos de regulamentos, serviços, produtos e demais atividades da organização alinhados ao negócio. Destacando a necessidade de uma atenção maior na entrega de serviço e ações dos usuários, que é onde a segurança se concretiza.

Figura 3 – Seqüência para a segurança ser realizada pelo usuário
Fonte: Edison Fontes, p. 89. 2011

2.1.2 Família ISO 27000

ISO/IEC 27000 - Sistema de Gerenciamento de Segurança - Explicação da série de normas, objetivos e vocabulários. Visando padronizar o processo de segurança da informação, criou-se a série ISO/IEC 27000, com normas e um código de boas práticas para implantação e manutenção da segurança da informação. A série ISO 27000 está de acordo com outros padrões de sistemas de gerência ISO, como ISO 9001 (Sistemas De Gerência Da Qualidade) e ISO 14001 (Sistemas De Gerência Ambiental).

As normas a seguir fazem parte da Família ISO/IEC 27000, onde as três normas principais, detalhadas a seguir, tratam específica e

independentemente, da tomada de decisão enquanto as outras normas dessa família são políticas auxiliares a fim de aperfeiçoar o tratamento com a segurança da informação. “Uma organização precisa identificar e gerenciar muitas atividades para funcionar efetivamente. Qualquer atividade que faz uso de recursos e os gerencia para habilitar a transformação de entradas em saídas pode ser considerada um processo. Freqüentemente a saída de um processo forma diretamente a entrada do processo seguinte.” (ABNT, 2005)

A seguir, uma breve explanação das normas e suas principais funções:

- **ISO/IEC 27001:2006** - Padrão para sistema de gestão da segurança da informação – Requisitos para implantar um Sistema de Gestão da Segurança da Informação – SGSI
- **ISO/IEC 27002:2005** - Esta Norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.
- **ISO/IEC 27003:2010** - Guia de Implantação de um Sistema de Gestão da Segurança da Informação.
- **ISO/IEC 27004:2009** - Gerenciamento de Métricas e Relatórios para um Sistema de Gestão de Segurança da Informação - Mostra como medir a eficácia do sistema de gestão de SI na corporação.
- **ISO/IEC 27005:2008** - Gestão de Riscos de Segurança da Informação.
- **ISO/IEC 27006:2007** - Requisitos para auditorias externas em um Sistema de Gerenciamento de Segurança da Informação.
- **ISO/IEC 27007:2011** - Referências para auditorias em um Sistema de Gerenciamento de Segurança da Informação.
- **ISO/IEC 27008:2011** - Auditoria nos controles de um SGSI - O foco são nos controles para implementação da ISO 27001.
- **ISO/IEC 27010:2012** - Gestão de Segurança da Informação para Comunicações Inter Empresariais- Foco na transparência entre empresas particulares e governamentais.
- **ISO/IEC 27011:2008** - Gestão de Segurança da Informação para empresa de Telecomunicações baseada na ISO 27002.

2.1.2.1 ISO 27001

Esta norma especifica os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Escalonando de forma estratégica os riscos de negócio e valorização dos ativos da organização, considerando segurança física, técnica, procedimental e de pessoas. “A especificação e implementação do SGSI de uma organização são influenciadas pelas suas necessidades e

objetivos, requisitos de segurança, processos empregados, tamanho e estrutura da organização.” (ABNT, 2005). Esta norma utiliza o modelo PDCA (*Plan-Do-Check-Act*), que significa Planejar, Fazer, Checar (Monitorar), Agir. Onde, no Planejamento é que se encontra a relação com as políticas de segurança da informação.

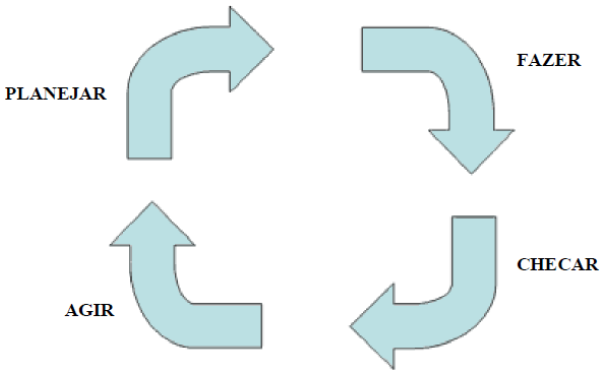


Figura 4 – PDCA – Sistemas de Gestão da Segurança da Informação
Fonte: http://pt.wikipedia.org/wiki/Ciclo_PDCA

2.1.2.2 ISO 27002

“É um conjunto completo de onze cláusulas (ou seções) de controle de segurança e 133 controles de segurança em forma que apóia e suporta a ISO 27001. Estes controles são os elementos que definem o que a norma considera importante para um processo, a fim de orientar a forma mais adequada de proteção da informação” (ABNT, 2005). As Normas ISO/IEC 27002 e ISO/IEC 27001 têm origem no Padrão Britânico, que em 1993 criou a Norma BS 7799, publicada pelo BSI (*British Standart International*). Até então, ainda sendo uma única norma, mas dividida em duas partes. No ano de 2000, a ISO (*International Organization for Standardization*) publica a norma ISO 17799, baseada na primeira parte, onde se tratava do código de conduta ou o guia de execução para a gestão da segurança da informação. Em 2005, a norma sofreu uma revisão, surgindo a ISO/IEC 17799:2005. Nesse mesmo período, foi criada a Família 27000. E como primeira norma, a segunda parte, onde continha os requisitos de auditoria para a certificação de um sistema de gestão de segurança da informação. Dando origem a ISO/IEC 27001:2005. Em 2007 a ISO/IEC 17799:2005 passou para o novo padrão e tornou-se a Norma ISO/IEC 27002:2005.

No Brasil elas foram traduzidas pela ABNT e são chamadas de NBR ISO/IEC 27001:2006 e NBR ISO/IEC 27002:2005. “Política de Segurança da Informação da organização protege a informação com a definição de controles ou grupos de controles. A Norma ISO/IEC 27002 apresenta 133 controles

divididos em 11 seções que devem ser consideradas e analisadas se serão considerados pela política da organização.” (ABNT, 2005)

a) Política de Segurança da Informação
b) Organizando a Segurança da Informação
c) Gestão de Ativos
d) Segurança em Recursos Humanos
e) Segurança Física e do Ambiente
f) Gestão das Operações e Comunicações
g) Controle de Acesso
h) Aquisição, Desenvolvimento e Manutenção e Sistemas de Informação
i) Gestão de Incidentes de Segurança da Informação
j) Gestão da Continuidade do Negocio
k) Conformidade

2.1.2.3 ISO 27005

Essa norma é responsável por todo ciclo de controle de riscos na organização, atuando junto à ISO 27001 em casos de certificação ou através da ISO 27002 em casos de somente implantação. Contribuindo para a capacidade de decisão da empresa na hora de identificar ameaças, probabilidades e vulnerabilidades de riscos. Segundo, Hori (2003), ameaça significa todo e qualquer evento ou incidente que possibilite explorar vulnerabilidade. Vulnerabilidade, por sua vez, é a fragilidade que compromete a segurança, concretizando a ameaça. Risco é a combinação da probabilidade (chance da ameaça se consolidar) de ocorrer um evento indesejado e suas possíveis conseqüências.

Risco = Impacto x Probabilidade.

A política de segurança da informação é encontrada na definição do contexto de escopo e limites que serão considerados no SGSI e conseqüentemente na gestão de riscos.

O surgimento dessa norma se deu no ano de 1995, com o título de AS/NZS 4360, criada para padronizar o processo de gestão de riscos da Austrália e Nova Zelândia. Em 2009, após treze anos de reajustes e percalços, a ISO publica sua versão chamada ISO 31000:2009 Gestão de Riscos – Princípios e diretrizes, publicada a versão em português pela ABNT no mesmo ano. Este norma é auxiliada por outras duas normas: ABNT ISO *GUIDE* 73:2009 – Vocábulos (termos genéricos) e ISO/IEC 31010:2009 – Técnicas de avaliação de Riscos (ABNT, 2009). Com base nos estudos desenvolvidos pela Norma ISO 31000:2009, foi criada a ISO 27005:2008. A diferença entre elas é

que a primeira tem uma concepção mais genérica e abrangente aos conceitos, definições e metodologias a todos os setores, enquanto a outra se baseia exclusivamente nas melhores práticas específicas da segurança da informação. Essas normas são distintas e uma não substitui a outra (ABNT, 2009).

2.2 A GOVERNANÇA CORPORATIVA

Segundo Coelho *et. al. (2010),* governança corporativa é o conjunto de processos, costumes, políticas, leis e instituições, baseado nos princípios da transparência, independência e prestação de contas (*accountability*), como meio para atrair investimentos para a organização que afetam o modo como uma empresa é administrada. Contribuindo para um desenvolvimento econômico sustentável.

Em 1995, um grupo de 36 pessoas, entre empresários, conselheiros, executivos, consultores e estudiosos, fundaram o Instituto Brasileiro de Conselheiros de Administração (IBCA). Com o intuito de colaborar com a qualidade da alta gestão das organizações brasileiras, fazendo com que elas mesmas atuassem afetivamente na continuação dos seus negócios. Porém, no começo, surgiram preocupações com relação a questões de propriedade, diretoria, conselho fiscal e auditoria independente. Em 1999, o Instituto passou a se denominar Instituto Brasileiro de Governança Corporativa (IBGC). Sendo referência em governança corporativa em toda a America Latina, contribuindo para o desempenho sustentável das organizações de forma transparente, independente, proativa, justa e responsável. Visando sanar as principais fragilidades das organizações e de seus sistemas de governança, auxiliando em fusões e aquisições de grandes companhias e o nivelamento de suas distinções, o IBGC criou o Código das Melhores Práticas de Governança Corporativa. Desde então, vem evoluindo e incorporando diversas atualizações e modificações, inicialmente divididas em três principais partes: Inovação, Detalhamento e Revisão/Enxugamento. Atualmente, subdivido em seis capítulos: Propriedade, Conselho de Administração, Gestão, Auditoria Independente, Conselho Fiscal, Conduta e Conflito de Interesses.

O IBGC, considerado Centro de Excelência em Governança Corporativa para a América Latina, Caribe e a África Lusófona, define a Governança Corporativa como: “Um sistema pelo qual as sociedades (empresas) são dirigidas e monitoradas, envolvendo os relacionamentos entre acionistas/cotistas, conselho e administração, diretoria, auditoria independente e conselho fiscal. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade.”

Empresas que possuem ações na bolsa de Valores, tal como a de Nova Iorque, tem por obrigação a elaboração estratégica de suas políticas de segurança da informação, por conta da exigência contida na Lei *Sarbane-Oxley*(SOX). Criada em 2002, pelos senadores americanos Michael Oxley e Paul Sarbanes, sansionada pelo Presidente George W. Bush, em reação aos escândalos de fraudes contábeis de grandes empresas dos EUA. Essa lei obriga a transparência, a fim de propor uma maior confiabilidade entre seus clientes, acionistas e colaboradores. A Lei visa a aprimorar a precisão das informações divulgadas pelas empresas e a aumentar as punições para eventuais desvios de conduta por parte dos executivos.

2.2.1 Governança de TI

O ambiente de tecnologia da informação tem por característica ser muito mais operacional que tático/estratégico dentro de uma organização.

"A governança de TI integra e institucionaliza boas práticas para garantir que a área de TI da organização suporte os objetivos de negócios" (Cobit 4.1, p. 7).

Governança de TI é uma ramificação da Governança Corporativa e orienta em como fazer uma boa gestão de TI, sendo uma prática que tem sido transmitida e compartilhada pelas empresas, por meios de mecanismos de controle e alinhamento da Tecnologia da Informação ao negócio da organização e o seu planejamento estratégico. Alinhando suas estratégias de negócios aos serviços de tecnologia, se garante a entrega dos processos de negócio operável e gerenciável, com qualidade e alta disponibilidade nos serviços de aplicação. "A Governança de TI é uma estrutura de relacionamentos e processos para dirigir e controlar a empresa a fim de alcançar os seus objetivos pela adição de valor, ao mesmo tempo em que equilibra riscos versus retorno sobre TI e seus processos" ISACA (2000).

Desde 1969, a Associação de Auditoria e Controle de Sistemas de Informação, ISACA, desenvolve padrões globais para auditorias de Sistemas de Informação, direcionando lideres de TI e negócios a maximizar o valor e gerenciar o risco relacionado à tecnologia da informação. A ISACA desenvolveu 16 guias, tituladas Normas de Auditoria de Segurança da Informação, visando definir o nível mínimo de desempenho aceitável exigido para dar resposta às responsabilidades profissionais estabelecidas no Código de Ética Profissional da ISACA. Entre os temas principais estão: Comércio Eletrônico; Ética e Padrões Profissionais; Materialidade da Auditoria; Governança de Ti E Irregularidades e Atos Ilegais.

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

Em 1992, o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) publicou a obra *Internal Control – Integrated Framework* para ajudar empresas e outras organizações a avaliar e aperfeiçoar seus sistemas de controle interno. Desde então, a referida estrutura foi incorporada em políticas, normas e regulamentos adotados por milhares de organizações para controlar melhor suas atividades visando o cumprimento dos objetivos estabelecidos. Segundo Coutinho (2009), existem alguns modelos de gestão de TI disponíveis no mercado que podem contribuir como base para uma boa administração, tais como: Processo CMMI (*Capability Maturity Model Integration*), à Gestão PMBOK (Project Management Body of Knowledge) e aos modelos de Governança: COBIT (Control Objectives for Information and Related Technology) e ITIL (Information Technology Infrastructure Library).

2.3 PRÁTICAS COBIT

"A Metodologia COBIT foi desenvolvida na década de 90 pelo ICASA e trata-se de um *framework*, ou guia de melhores práticas, mais utilizado no mundo em termos de Governança de TI. O COBIT fornece um conjunto detalhado de controles e técnicas de controle para o ambiente de gestão de sistemas de informação, chamados de objetivos de controle como: gerenciamento de incidentes, problemas, segurança da informação, indicadores, auditoria externa entre outros objetivos para que se possa garantir o controle das informações que se encontram em sistemas de informação" (COBIT, 2007).

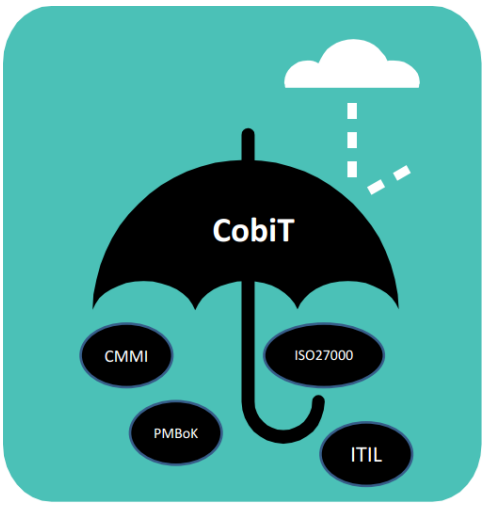


Figura 5 – Divisão COBIT e TI para cobrir toda a Governança de TI
Fonte: Meyer, 2009

O *Framework* COBIT determina que "É responsabilidade da gestão salvaguardar todos os ativos da empresa. Para cumprir com essa responsabilidade e também alcançar as expectativas, a gestão deve estabelecer um sistema adequado de controle interno".

Para atender aos objetivos de negócios, as informações precisam se adequar a certos critérios de controles, aos quais o CobiT denomina necessidades de informação da empresa. Baseado em abrangentes requisitos de qualidade, guarda e segurança.

A orientação aos processos está definida em 34 processos, divididos em 4 domínios:

Planejamento e Organização (PO) – Estratégias, táticas e aspectos para melhor contribuição da TI para alcançar os objetivos de negócios;

Aquisição e Implementação (AI) – Estratégias de TI para a identificação de soluções de TI, necessidades de desenvolvimento ou aquisição de tecnologia, implementação e integração com os processos de negócios;

Entrega e Suporte (DS) – Aborda as estratégias para entrega dos serviços requisitados, incluindo entrega do serviço, gerenciamento de dados e facilidades operacionais;

Monitoração e Avaliação (ME) – Aborda o gerenciamento de desempenho, monitoração de controles internos e provê a governança, visando avaliar a qualidade dos processos e conformidade com os requisitos de controle.

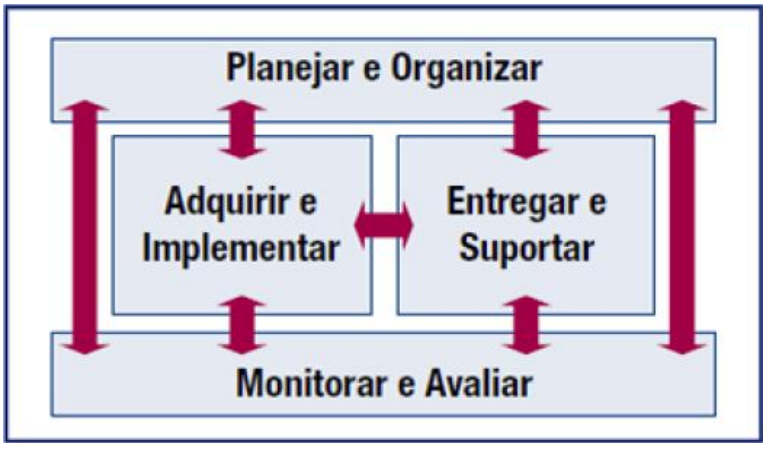


Figura 6 – Os quatro domínios inter-relacionados do COBIT
Fonte: COBIT, Edição 4.1, 2007

A definição dos objetivos acontece de cima para baixo, do negócio para a atividade:

- Objetivos de Negócio: definem os objetivos da organização, é a parte estratégica.
- Objetivos de TI: são derivados dos objetivos do negócio e definem o que o negócio espera da TI.
- Objetivos de Processo: definem o que os processos de Ti precisam fazer e entregar para atender os objetivos de TI.
- Objetivos das Atividades: Definem o que precisa ser feito dentro de cada processo.

Além de definir os objetivos, que são os resultados esperados, é preciso verificar se os resultados foram ou serão alcançados. O COBIT possui dois tipos de indicadores estratégicos:

- Medidores de Resultado: Indica se um processo alcançou seu resultado esperado, que são os objetivos.
- Indicadores de Desempenho: Indicado para medir o progresso em relação ao objetivo que se quer alcançar.

2.3.1 Nível de Maturidade

No CMMI (*Capability Maturity Model Integration* - Modelo Integrado de Capacitação e Maturidade), a maturidade é da empresa e não do processo. O modelo de maturidade do COBIT mede o desempenho ou maturidade de cada processo de TI, permitindo identificar o estágio atual médio do mercado e assim comparar com a maturidade da organização. Sendo possível criar uma meta de aprimoramento da empresa para determinar até onde a instituição quer chegar.

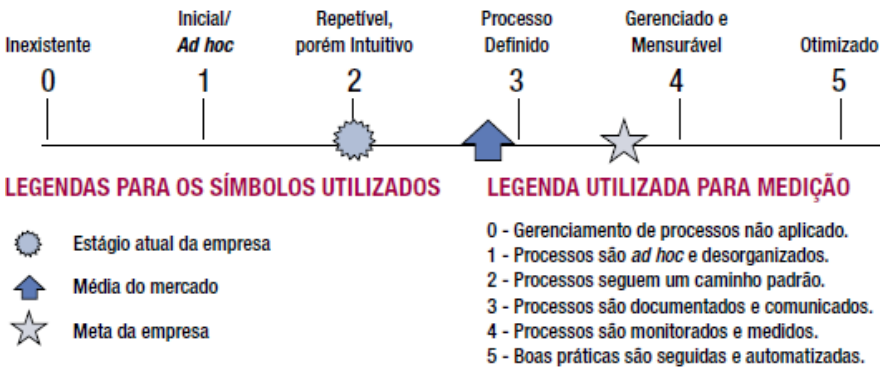


Figura 7 – Representação Gráfica dos Modelos de Maturidade
Fonte: COBIT, Edição 4.1, 2007

2.4 PRÁTICAS ITIL

O ITIL – *Information Technology Infrastructure Library* – foi desenvolvido pelo governo britânico no final da década de 80 e provou que possui um estrutura útil em todos os setores tendo em vista a sua adoção em várias empresas de gerenciamento de serviços. O ITIL tem como foco principal, a operação e a gestão da infra-estrutura de tecnologia na organização, incluindo todos os assuntos que são importantes no fornecimento dos serviços de TI. Nesse contexto, o ITIL considera que serviço de TI é a descrição de um conjunto de recursos de TI. Os serviços de suporte de ITIL auxiliam no atendimento de uma ou mais necessidades do cliente, apoiando, desta forma, aos seus objetivos de negócios.

O Princípio básico do ITIL é o objeto de seu gerenciamento: a infra-estrutura de TI e o fornecimento de qualidade de serviço aos clientes de TI com custos justificáveis, isto é, relacionar os custos dos serviços de tecnologia incorporando valor estratégico ao negocio. A OGC (2007) dividiu o seu material para o ITIL V3 em cinco livros:

1. Service Strategy (Estratégias de serviços);
2. Service Design (Desenho de serviços);
3. Service Transition (Transição de serviços);
4. Service Operation (Operação de serviços);
5. Continual Services Improvement (Melhoria contínua de serviços).

O ITIL é uma estrutura voltada para o gerenciamento de serviço. Neste contexto, a segurança da informação aparece como uma função do *Service Design* (Desenho de Serviços), titulado como função de Gerenciamento de Segurança de Informação.

2.5 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Gestão de Riscos é um elemento central que faz parte do planejamento estratégico da organização e deve ser praticado por todos os níveis da administração, sendo parte integrante da Segurança da Informação. “Em um SGSI, a definição do contexto, a análise/avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco, fazem parte da fase planejar” (ABNT, 2008, p. 6). “Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e aplicada tanto à implementação quanto à operação cotidiana de um SGSI” (ABNT, 2008, p. 3). Segundo a NBR ISO/IEC 27005 (2008), podemos classificar os eventos da gestão de segurança da informação:

Vulnerabilidade - Vulnerabilidade que expõe riscos a eventos imprevistos e indesejáveis a empresa. É a fraqueza ou deficiência de um ou mais de ativos na infraestrutura da organização que pode ser explorada por uma ou mais ameaças. Isso permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade. Os principais tipos de vulnerabilidades existentes são: Físicas, naturais, hardware, software, mídias, comunicação ou humanas. Tais como: falhas em softwares, sistemas não atualizados, erro de configuração, uso indevido e erro humano, serviços habilitados e não utilizados, políticas não aplicadas, senhas fracas, autenticação fraca, ausência de controle de acesso físico.

a) Ameaça - Ameaça é a causa potencial de um incidente, por meio da exploração de vulnerabilidades, que pode resultar em danos para um sistema ou organização. Causado por um agente de forma acidental, natural ou proposital, incentivado por um motivo que pode afetar um ambiente, sistema ou ativo de informação. As ameaças podem ser divididas nos seguintes grupos:
   - Naturais: incêndios, enchentes, terremotos, tempestades, maremotos, aquecimento, poluição.
   - Involuntárias: falta de energia, umidade, temperatura do local dos servidores, funcionário sem treinamento.
   - Voluntárias: hackers, invasores, espiões, ladrões, funcionários descontentes. Por meio de varredura de portas, coleta de dados trafegados na rede, ataque por negação de serviço, vírus.

b) Incidente- Evento decorrente da ação de uma am eaça, que explora uma ou mais vulnerabilidades.

c) Impacto - Impacto é a abrangência dos danos causados por um incidente ou conseqüência de um ataque.

d) Risco - Risco é um evento futuro identificado, ao qual é possível associar uma probabilidade de ocorrência. Incerteza é evento futuro identificado, ao qual não é possível associar uma probabilidade de ocorrência. Risco é a probabilidade de ameaças explorarem vulnerabilidades, sendo medido através da probabilidade de que uma ameaça pode acontecer e o dano que pode ser gerado à empresa.

RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Ativo ou custo do evento)

2.5.1 Gerenciamento de Riscos

Segundo o IBGC, “Gerenciamento de riscos: o Conselho de Administração deve assegurar-se de que a Diretoria identifique preventivamente – por meio de sistema de informações adequado – e liste os principais riscos aos quais a sociedade está exposta, sua probabilidade de ocorrência, bem como as medidas e os planos adotados para sua prevenção ou minimização”.

2.5.1.1 Identificação e Classificação dos Riscos

Podemos classificar os Riscos quanto a origem, natureza e tipo do risco ou evento.

a) Origem dos Riscos

Segundo o IBGC, a classificação quanto à origem dos eventos é associada basicamente em riscos externos e internos:

- **Riscos Externos:** ocorrências associadas ao ambiente macroeconômico, político, social, natural ou setorial em que a organização opera. A organização, em geral, não consegue intervir diretamente sobre estes eventos e terá, portanto, uma ação predominantemente reativa.
- **Riscos Internos:** eventos originados na própria estrutura da organização, pelos seus processos, seu quadro de pessoal ou de seu ambiente de tecnologia. A organização pode e deve, em geral, interagir diretamente com uma ação pró-ativa.

b) Natureza dos Riscos

Da mesma forma, se torna relevante classificar a natureza dos riscos, em função das áreas da organização que são afetadas pelos eventos:

- **Riscos Estratégicos -** Os riscos estratégicos estão associados à tomada de decisão da alta administração e podem gerar perda substancial no valor econômico da organização ao não atingir suas metas. Os riscos estratégicos geralmente são externos.
- **Riscos Operacionais -** Os riscos operacionais estão associados à possibilidade de ocorrência de perdas (de produção, ativos, clientes, receitas) resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos

externos como catástrofes naturais, fraudes, greves e atos terroristas.

- **Riscos Financeiros (mercado, crédito e liquidez) -** são os riscos relacionados às operações financeiras da organização como encargos financeiros altos, fluxo de caixa instável ou garantias insuficientes.

c) Tipos de Riscos

Visando assegurar a definição descrição ampla dos tipos de risco e uma linguagem comum de riscos dentro da organização, o IBGC classifica os riscos em 3 tipos básicos:

- **Tecnologia:** representado por falhas, indisponibilidade ou obsolescência de equipamentos e sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, erros ou fraudes.
- **Ambiental:** catástrofes ou desastres ambientais, contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos.
- **Conformidade:** cumprir com a legislação e/ou regulamentação externa, aplicáveis ao negócio e às normas e procedimentos internos, decorrente da aplicação da legislação trabalhista, tributária, fiscal, referentes a relações contratuais, regulamentação de mercado e de prestação de serviços.

2.5.2 Gerenciamento de Operações

De acordo com *HORI*(2003), a segurança da informação deve identificar os riscos e vulnerabilidades das operações de negócio da empresa e implementar as devidas soluções de segurança, não só através da tecnologia, mas também, de processos e de pessoas. Essa área pode ser subdivida em:

- Arquitetura de segurança
- Segurança das operações
- Telecomunicações
- Segurança física
- Desenvolvimento de sistemas
- Resposta aos incidentes

2.5.2.1 Arquitetura de Segurança

Segundo (VALLABHANENI, 2002 *apud HORI, 2003), a* arquitetura de segurança do ambiente computacional refere-se a um conjunto de estruturas e aos detalhes que tratam das questões de segurança da informação e controles, em todos os níveis técnicos e operacionais necessários para o funcionamento

das diversas áreas de negócio. A arquitetura de segurança está envolvida com os sistemas operacionais, hardware, protocolos utilizados nas redes, circuitos e programas de sistema de operações. O protocolo *Internet Protocol Security – IPSEC* é projetado para oferecer segurança de alta qualidade para o tráfego da Internet e interoperabilidade, baseado em criptografia para *Internet Protocol – IP*v4 e *IP*v6.

2.5.2.2 Segurança das Operações

A segurança das operações é utilizada para identificar os controles sobre o hardware, as mídias e sobre os operadores com acesso privilegiado a esses recursos.

Segundo HORI (2003), as atividades relativas à segurança das operações:

- **Segregação das funções** - deve existir para garantir que nenhum indivíduo e/ou área desempenhe um processo completo como geração, entrada, autorização, verificação ou distribuição de dados.

- **Administração do antivírus** - Controles devem ser adotados para evitar a introdução de vírus de computador no ambiente interno da empresa. Atualizações constantes na lista de vírus devem ser realizadas, evitando assim que a empresa se torne suscetível ao ataque.

- **Procedimentos de *backup*** - As empresas deverão possuir procedimentos adequados para geração e retenção das mídias de *backup* e dos sistemas utilizados para geração dessas informações. A existência de mídias de *backup* é crucial para continuidade dos negócios caso ocorram incidentes de segurança.
  A decisão sobre a periodicidade de realização de *backup* de determinados arquivos está baseado no custo de realizar o *backup*, *versus*: o custo de falha; a capacidade de recriar o arquivo sem um *backup*; e tempo necessário para realizar uma cópia de segurança.

- **Inventário dos ativos** - O inventário de todos os *hardwares* de computador, como processadores, monitores, *notebooks*, *modems*, equipamentos de telecomunicação, roteadores, *fax*, PABX, devem ser registrados no inventário de ativos físicos. Esse inventário de ativos da informação deverá ser revisado sempre que esses *hardwares* forem removidos, descartados, realocados, atualizados ou sofrerem qualquer outro tipo de alteração.

- **Documentação das Operações** - É necessário formalizar todos os procedimentos operacionais executados por suas áreas de negócio. Entretanto, num primeiro momento, essa atividade deverá ser priorizada nas áreas onde há o manuseio de informações sensíveis e a utilização de um volume muito grande de mão de obra terceirizada, buscando dessa forma, minimizar a dependência desses terceiros.

- **Manuseio e destruição de mídias** - Devem-se elaborar Políticas, Normas e Procedimentos de Segurança referentes ao armazenamento e ao descarte das mídias que contenham informações de alta criticidade. Adicionalmente, a adoção de dispositivos apropriados de armazenamento de descarte é necessária.

- **Monitoramento das trilhas de auditoria** - são gravadas em arquivos de *log*, auxiliam na detecção de violações de segurança, de problemas de desempenho e de falhas nos sistemas. Em virtude de os arquivos de *log* serem recursos passivos, visto que eles somente coletam dados e não tomam nenhuma ação, sua maior utilidade está na detecção e intimidação de ações consideradas impróprias.

- **Análise de risco** - As empresas devem utilizar a análise de risco para todas as informações e/ou sistemas, incluindo aqueles que ainda estão em fase de desenvolvimento. Os riscos oferecidos ao negócio, associados aos sistemas e às informações, devem ser avaliados usando-se um método formal de análise de risco, o qual deve ser documentado, flexível, de fácil compreensão, aprovado pela alta administração e periodicamente revisado, para assegurar que ele atinja as necessidades de negócio.

2.5.2.3 Telecomunicações

Esta área aborda os métodos de transmissão, as formas de tráfego de informações e as medidas de segurança utilizadas para fornecer integridade, disponibilidade, autenticação e confiabilidade para as transmissões ocorridas, utilizando redes de comunicação pública e privada. Para a segurança desta área, são necessários: modems, PABX, *firewalls*, cabeamentos estruturados, VPN, *wireless,* segurança em email, assinatura digital, IDS. As novas gerações desses produtos incorporam diversas funcionalidades, passando por filtragem de tráfego (firewall), comunicação segura (VPN), detecção e prevenção de intrusão (IDS/IPS), antivírus/anti-spam, filtro de conteúdo, autenticação e controle de acesso.

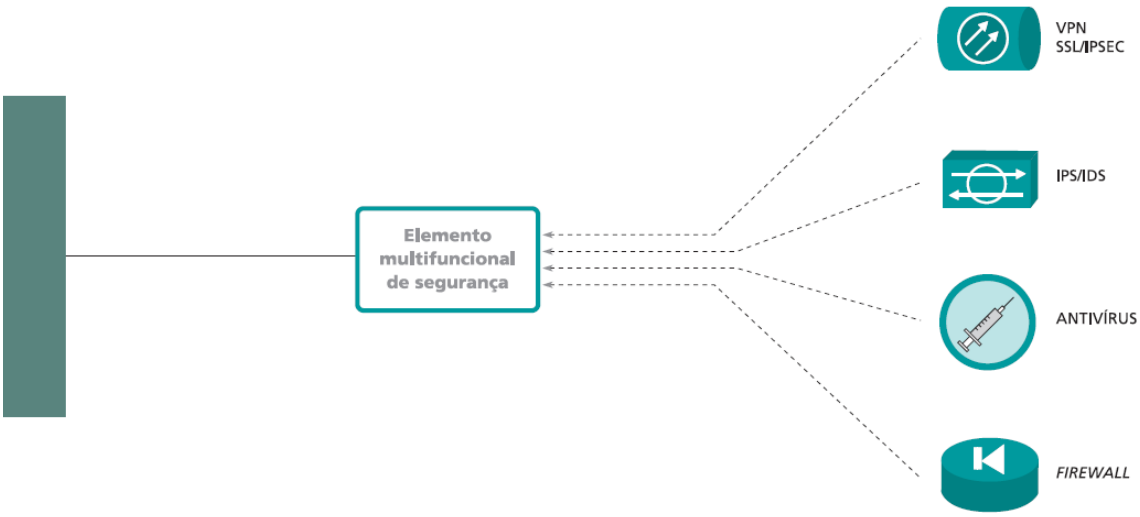


Figura 8: Elemento multifuncional de segurança
Fonte: Promon (2005)

2.5.2.4 Segurança Física

Este tópico estabelece todos os requisitos de segurança física a que a empresa deverá atentar, desde procedimentos até a adoção de dispositivos específicos, como detectores de incêndio, sensores, câmeras. Para isto são necessários:

- Segurança das Áreas Restritas - como acesso ao Centro de Processamento de Dados (CPD) ou outras áreas consideradas críticas.
- Controle de Acesso Físico - devem cobrir toda a área em que o cabeamento da *Local Area Network (LAN)*, nos locais onde ocorrem os serviços de suporte e a operação como cabine de energia elétrica, sala com os equipamentos de ar condicionado, sala com os *links* de comunicação e todos os outros elementos requeridos para a operação dos sistemas. Os controles de acesso físicos restringem a entrada e a saída das pessoas através de dispositivos eletrônicos e mídias.
- Controles Preventivos do Sistema de Suporte Ambiental - Os sistemas e as pessoas que os operam necessitam de um ambiente razoavelmente bem controlado. Deve ser controlada as falhas relacionadas ao sistema de ventilação (ar-condicionado), à eletricidade e aos outros dispositivos geralmente causarão danos e até mesmo a interrupção nos serviços, podendo ainda danificar o funcionamento dos equipamentos críticos.

A segurança das redes vem se tornando cada vez mais importante. As redes convergentes transportam, hoje em dia, informações relevantes para todos os aspectos de um negócio, desde dados de extrema criticidade, como é o caso de informações financeiras, até a comunicação tradicional de voz, vídeo e dados. Além de desempenharem sua funcionalidade tradicional de comunicação, as redes passam a ter também um papel de destaque no combate a ameaças à segurança dos dados e aplicações.

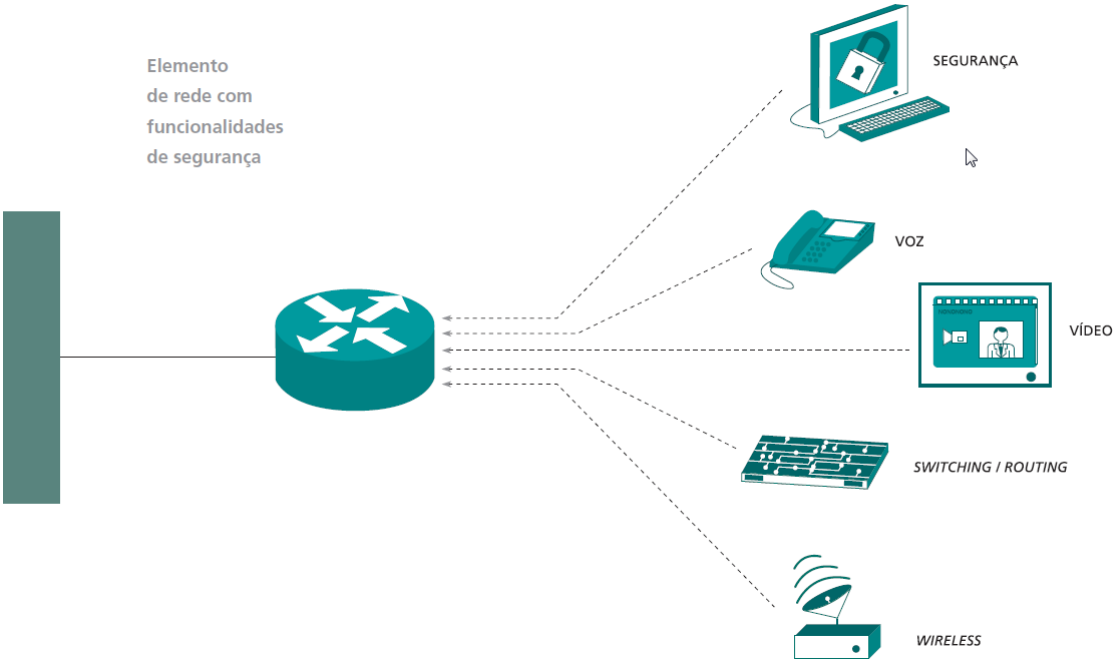


Figura 9: Elemento de rede com funcionalidades de segurança
Fonte: Promon (2005)

2.5.2.5 Desenvolvimento e Manutenção de Sistemas

São os controles incluídos dentro dos sistemas e aos aspectos a serem atentados durante o ciclo de desenvolvimento e de manutenção dos sistemas: codificação segura, segregação de ambientes, metodologia e projeto de desenvolvimento, estabelecimento de acordo de nível de serviço com os prestadores, controle de versão, testes de qualidade do sistema, documentação de segurança, certificação de um produto ou sistema.

2.5.2.6 Resposta a Incidentes

Desenvolve os planos de continuidade que permitam à instituição não só continuar a realização de seus negócios em situação de contingência, como também gerenciar os riscos de possíveis interrupções e retornar o funcionamento normal das operações.

a) Planos de Contingência

São desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencente ao escopo, definido em detalhes os procedimentos a serem executados em estado de contingência. É acertadamente subdivido em três módulos distintos e complementares que tratam especificamente de cada momento vivido pela empresa.

b) Plano de Administração de Crise

Este documento tem o propósito de definir passo – a – passo o funcionamento das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem que definir os procedimentos a serem executados pela mesma equipe no período de retorno à normalidade. O comportamento da empresa na comunicação do fato à imprensa é um exemplo típico de tratamento dado pelo plano.

c) Plano de Continuidade Operacional

Este documento tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, conseqüentemente, os impactos potenciais ao negócio. Orientar as ações diante da queda de uma conexão à Internet exemplifica os desafios organizados pelo plano.

d) Plano de Recuperação de Desastres

Este documento tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação.

É fator crítico de sucesso estabelecer adequadamente os gatilhos de acionamento para cada plano de contingência. Estes gatilhos são parâmetros de tolerância usados para sinalizar o início da operacionalização da contingência, evitando acionamentos prematuros ou tardios. Dependendo das características do objeto da contingência, os parâmetros podem ser: percentual de recurso afetado, quantidade de recursos afetados, tempo de indisponibilidade, impactos financeiros etc.

2.5.3 Auditoria de Sistemas

Segundo o Relatório do Comitê de Conceitos Básicos de Auditoria da Associação Americana de Contabilidade, a auditoria é um processos sistemático de obter e avaliar evidências enfocando afirmações sobre ações e eventos econômicos para avaliar o grau de correspondência entre estas afirmações e os critérios estabelecidos para comunicação dos resultados aos interessados.

Pode-se classificar a auditoria em três tipos:

- Auditoria de demonstrações financeiras: envolve a análise das evidências sobre as demonstrações financeiras de uma empresa, com o objetivo de opinar se tais demonstrações foram desenvolvidas obedecendo a um critério estabelecido.
- Auditoria de conformidade (*compliance*): envolve a análise das evidências de algumas atividades financeiras ou operacionais de uma empresa, com o propósito de verificar se estas estão em conformidade com as condições e regulamentos específicos ao assunto.
- Auditoria operacional: compreende a análise das evidências sobre a eficiência e a eficácia das atividades operacionais de uma empresa em relação a objetivos específicos.

Na auditoria interna é feita a averiguação de todos os procedimentos internos e políticas definidas pela empresa por um auditor que fica constantemente na empresa e, normalmente, trabalha junto à diretoria executiva ou à presidência. Enquanto na auditoria externa ou auditoria independente, o auditor externo trabalha de forma independente, em parceria com o auditor interno, testa a eficiência dos sistemas utilizados e a confiabilidade dos registros contábeis.

2.5.4 Modelo de Gestão de Riscos

Segundo a NBR ISO/IEC 27005, para um funcionamento adequado do SGSI é importante que a gestão de riscos e a política de segurança da informação sejam elementos que estejam bem definidos e explícitos. No contexto da gestão de riscos, a política de segurança da informação é considerada na fase de definição do contexto, mais especificamente na definição de escopo e limites. “Convém que a organização defina o escopo e os limites da gestão de riscos de segurança da informação” (ABNT, 2008).

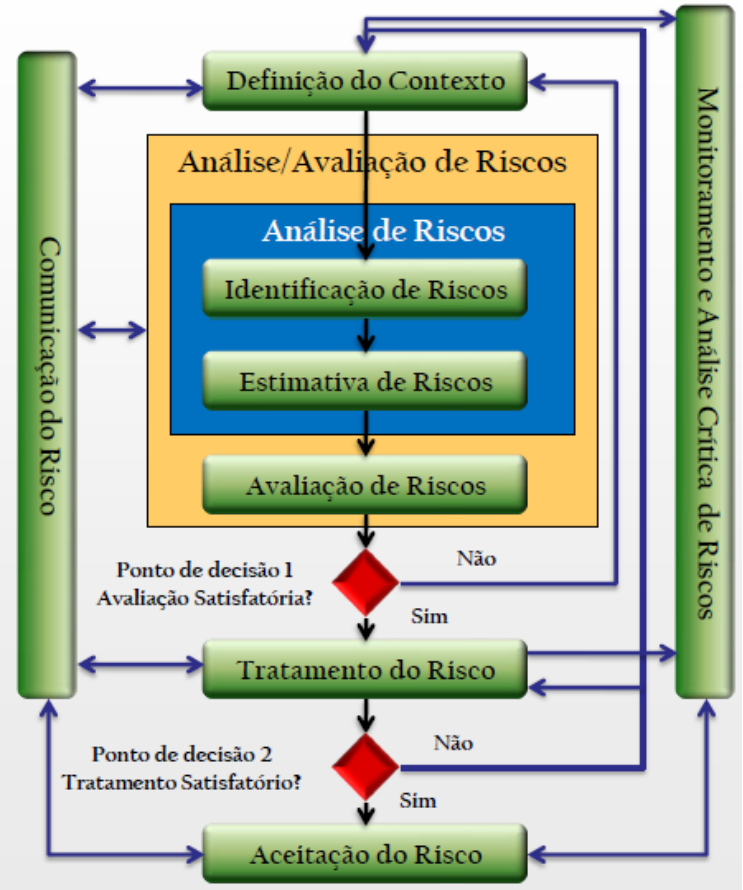


Figura 10: Processo de gestão de riscos de segurança da informação
Fonte: ABNT (2008)

Em conjunto com a Norma ISO/IEC 27001, o Processo do SGSI propõe o ciclo de melhoria contínua PDCA para o tratamento na Gestão de Riscos.

Tabela 1 – Alinhamento do processo do SGSI e gestão de riscos de SI

Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Análise/avaliação de riscos Plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Fonte: ABNT (2008)

A norma ABNT ISO/IEC 27005 segmenta o processo de gestão de risco de segurança da informação da seguinte maneira:

a) Definição do contexto

Dentro do processo, a definição do contexto é responsável pela definição do ambiente, escopo, critérios de avaliação, limites, entre outras definições. Esta etapa é essencial para realizar a gestão de risco a conhecer todas as informações sobre a organização. Esta etapa indica os critérios básicos, escopo e limites e as responsabilidades para o processo de gestão de riscos.

b) Análise/avaliação de riscos de segurança da informação

A próxima iteração é de análise e avaliação de risco, que permitirá a identificação dos riscos e a determinação das ações necessárias para reduzir o risco a um nível aceitável.

A norma descreve todo o processo de análise e avaliação dos riscos de segurança da informação, detalhando:

- Identificação de ativos.
- Identificação de ameaças.
- Identificação de controles existentes.
- Identificação das vulnerabilidades.
- Identificação das conseqüências.
- Estimativa dos riscos (quantitativa, qualitativa).
- Avaliação da probabilidade dos incidentes.
- Estimativa do nível de risco.

De acordo com a ABNT NBR ISO/IEC 27005 “A análise/avaliação de riscos determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades aplicáveis existentes, identifica os controles existentes e seus efeitos no risco identificado, determina as conseqüências possíveis, prioriza os riscos derivados e ordena-os de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto”.

c) Tratamento do risco de segurança da informação

A partir dos resultados obtidos na análise e avaliação do risco são definidos os controles necessários para o tratamento do risco, a norma ABNT NBR ISO/IEC 27001 especifica os controles que deverão ser implementados. O processo de tratamento dos riscos de segurança da informação é feito em quatro ações com:

- Mitigá-lo - através da aplicação de controles específicos;
- Transferi-lo - através de atividades como um seguro;
- Aceitá-lo - simplesmente tomando o conhecimento, mas sem adoção de medidas de controle;
- Evitá-lo - executando outra atividade, tomando outro caminho, não utilizando o item.

d) Aceitação do risco de segurança da informação

Assegura os riscos aceitos pela organização, ou seja, os riscos que por algum motivo não serão tratados ou serão tratados parcialmente. São os chamados riscos residuais, cujo enquadramento nesta categoria deverá ser formalmente registrado.

e) Comunicação do risco de segurança da informação

Nesta etapa é feita a comunicação do risco e da forma como será tratado, para todas as áreas operacionais e seus gestores. A comunicação eficaz e a inter-relação das partes envolvidas no tratamento dos riscos podem ter um impacto significativo nos processos de decisão da gestão de riscos em segurança da informação.

f) Monitoramento e análise crítica de riscos de segurança da informação

São as atividades de acompanhamento dos resultados, implementação dos controles e de análise crítica para a melhoria contínua identificando possíveis mudanças no contexto da organização no processo de gestão de riscos.

2.5.5 Método MARAT

Segundo Marques (2005), o Método de Análise de Riscos e Acidentes de Trabalho – MARAT, permite hierarquizar de modo racional a prioridade de eliminação, minimização e/ou controle do risco, dando-nos uma informação clara acerca do seu grau de probabilidade de ocorrência e magnitude dos danos (conseqüências).

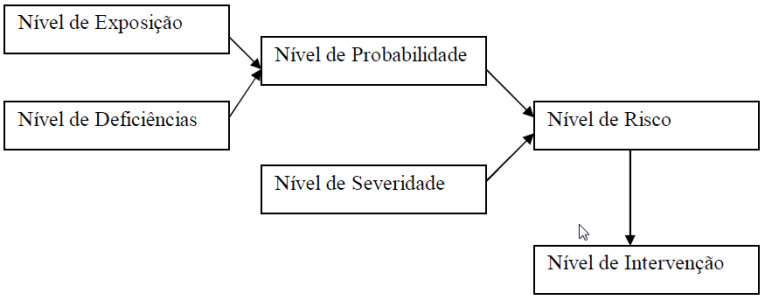


Figura 11: Fluxograma do desenvolvimento do método
Fonte: MARAT (2005)

2.5.5.1 Nível de Deficiência (ND)

Designa-se por nível de deficiência (ND), ou nível de ausência de medidas preventivas, a magnitude esperada entre o conjunto de fatores de risco considerados e a sua relação causal direta com o acidente. A tabela, que se segue, enquadra-nos a avaliação num determinado nível de deficiência:

Tabela 2 – Nível de Deficiência

Nível de Deficiência	ND	Significado
Aceitável (A)	1	- Não foram detectadas anomalias. - O perigo está controlado.
Insuficiente (I)	2	- Foram detectados factores de risco de menor importância. - É de admitir que o dano possa ocorrer algumas vezes.
Deficiente (D)	6	- Foram detectados alguns factores de risco significativos. - O conjunto de medidas preventivas existentes tem a sua eficácia reduzida de forma significativa.
Muito Deficiente (MD)	10	- Foram detectados factores de risco significativos. - As medidas preventivas existentes são ineficazes. - O dano ocorrerá na maior parte das circunstâncias.
Deficiência Total (DT)	14	- Medidas preventivas inexistentes ou desadequadas. - São esperados danos na maior parte das situações.

Fonte: PEDRO(2006)

2.5.5.2 Nível de Exposição (NE)

O nível de exposição é uma medida que traduz a freqüência com que se está exposto ao risco. A tabela, que se segue, enquadra-nos a avaliação num determinado nível de exposição:

Tabela 3 – Nível de Exposição

Nível de Exposição	NE	Significado
Esporádica	1	- Uma vez por ano ou menos e por pouco tempo (minutos).
Pouco Frequente	2	- Algumas vezes por ano e por período de tempo determinado.
Ocasional	3	- Algumas vezes por mês.
Frequente	4	- Várias vezes durante o período laboral, ainda que com tempos curtos – várias vezes por semana ou diário.
Continuada Rotina	5	- Várias vezes por dia com tempo prolongado ou continuamente.

Fonte: PEDRO(2006)

O nível de probabilidade é determinado em função das medidas preventivas existentes e do nível de exposição ao risco. A tabela compara o produto do nível de deficiência com o nível de exposição:

Tabela 4 – Produto da deficiência com a exposição

			Nível de Exposição				
			Esporádica	Pouco Frequente	Ocasional	Frequente	Continua
			1	2	3	4	5
Nível de Deficiência	Aceitável	1	1	2	3	4	5
	Insuficiente	2	2	4	6	8	10
	Deficiente	6	6	12	18	24	30
	Muito Deficiente	10	10	20	30	40	50
	Deficiência Total	14	14	28	42	56	70

Fonte: PEDRO(2006)

A tabela demonstra o nível de probabilidade de se ocorrer o evento:

Tabela 5 – Nível de Probabilidade

Nível de Probabilidade	NP	Significado
Muito Baixa	[1;3]	Não é de esperar que a situação perigosa se materialize, ainda que possa ser concebida.
Baixa	[4;6]	A materialização da situação perigosa pode ocorrer.
Média	[8;20]	A materialização da situação perigosa é passível de ocorrer pelo menos uma vez com danos.
Alta	[24;30]	A materialização da situação perigosa pode ocorrer várias vezes durante o período de estudo.
Muito Alta	[40;70]	Normalmente a materialização da situação perigosa ocorre com frequência.

Fonte: PEDRO(2006)

Nível de Severidade (NS)

O nível de severidade do dano refere-se ao dano mais grave que é razoável esperar de uma ocorrência envolvendo o perigo avaliado:

Tabela 6 – Nível de Severidade

Níveis de Severidade	NS	Significado	
		Danos Pessoais	Danos Materiais
Insignificante	10	Não há danos pessoais	Pequenas perdas materiais nas empresas
Leve	25	Pequenas lesões que não requerem hospitalização. Apenas primeiros socorros	Reparação dos danos, sem paragem da actividade das empresas.
Moderado	60	Lesões com incapacidade transitória. Requerem tratamento médico	Requer a paragem das actividades para efectuar a reparação nas empresas
Grave	90	Lesões graves que podem ser irreparáveis.	Destruição parcial do sistema em estudo (reparação complexa e onerosa)
Mortal ou catastrófico	155	Um morto ou mais. Incapacidade total ou permanente	Destruição de um ou mais sistemas (difícil renovação / reparação).

Fonte: PEDRO(2006)

2.5.5.3 Nível de Risco (NR)

O nível de risco será o resultado do produto do nível de probabilidade pelo nível das conseqüências NR=NP x NS e que pode apresentar-se na tabela seguinte:

Tabela 7 – Nível de Risco

			Não é de esperar que o risco se materialize		A materialização do risco pode ocorrer.		A materialização do risco é passível de ocorrer		A materialização do risco pode ocorrer várias vezes durante o período de actividades		A materialização ocorre com frequência.	
Pessoas	**Material**	**NP / NS**	**1 a 3**		**4 a 6**		**8 a 18**		**24 a 30**		**40 a 70**	
Não há danos pessoais.	Pequenas perdas de material.	**10**	10	30	40	60	80	180	240	300	400	700
Pequenas lesões que não requerem hospitalização.	Reparação sem paragem das actividades.	**25**	25	75	100	150	200	450	600	750	1000	1750
Lesões com incapacidade temporária.	Requer a paragem das actividades para efectuar a reparação.	**60**	60	180	240	360	480	1080	1440	1800	2400	4200
Lesões graves que podem ser irreparáveis.	Destruição parcial do sistema em estudo (reparação complexa e onerosa).	**90**	90	270	360	540	720	1620	2160	2700	3600	6300
Um morto ou mais. Incapacidade total ou permanente.	Destruição de um ou mais sistemas (difícil renovação / reparação).	**155**	155	465	620	930	1240	2790	3720	4650	6200	10850

Fonte: PEDRO(2006)

2.5.5.6 Nível de Intervenção ou de Controle (NC)

O nível de controle pretende dar uma orientação para implementar programas de eliminação ou redução de riscos, atendendo à avaliação do custo/eficácia:

Tabela 8 – Nível de Controle

Nível de Controlo	NC	Significado
I	3600 a 10850	- Situação critica. - Intervenção imediata. - Eventual paragem imediata. - Isolar o perigo até serem adoptadas medidas de controlo permanentes
II	1240 a 3100	- Situação a corrigir. - Adoptar medidas de controlo enquanto a situação perigosa não for eliminada ou reduzida.
III	360 a 1080	- Situação a melhorar. - Deverão ser elaborados planos, programas ou procedimentos documentados de intervenção
IV	90 a 300	- Melhorar se possível justificando a intervenção
V	10 a 80	- Intervir apenas se uma analise mais pormenorizada o justificar

Fonte: PEDRO(2006)

2.5.5.7 Definição da aceitabilidade dos riscos avaliados

O critério utilizado para definir a aceitabilidade ou não aceitabilidade é o seguinte: Para valores de controle (NC) iguais ou inferiores a 300, consideraram-se os riscos aceitáveis. Para valores do controle (NC) iguais ou superiores a 360, consideraram-se os riscos não aceitáveis, o que implica que devem ser desencadeadas medidas no sentido de eliminá-los ou reduzir ao mínimo possível. Onde:

Aceitáveis - Todos os riscos com o Nível de Controle IV e V.

Inaceitáveis - Todos os riscos com o Nível de Controle III, II e I.

3 ESTUDO DE CAMPO

Este capítulo apresentará o levantamento do cenário atual, propondo uma implantação de melhoria da segurança. A proposta de melhoria ou implantação deverá contemplar as propriedades vistas (confidencialidade, integridade e disponibilidade), aplicadas aos estados da informação (processamento, armazenamento e transmissão) descrevendo as medidas (Política e Procedimentos, Tecnologia, Educação, Treinamento e Conscientização).

3.1 POLITICA DA EMPRESA

A MASISA reconhece a informação como um ativo intangível de alto valor, sendo ela: escrita, impressa, armazenada, apresentada em meios audiovisuais, falada, em ou por meios eletrônicos.

A informação se considera relevante para a competitividade, continuidade operacional, comercial e financeira.

Toda informação da organização tem aspectos confidenciais, de integridade e disponibilidade, o que constitui um bem. Reconhece-se toda a ameaça relativa à sua segurança como um fato que pode impactar nos negócios.

Os recursos destinados a resguardar a segurança da informação são:

Avaliação de riscos de segurança, para determinar e zelar pela vulnerabilidade de ativos, probabilidades de ocorrência de perda e seus impactos.

Legais, normativos, regulamentares e contratuais, os quais devem ser cumpridos por toda a organização e os que interagem direta ou indiretamente com ela.

Princípios, objetivos e requisitos para o processamento da informação criados com o propósito de amenizar qualquer oportunidade de perda em todos os países e divisões.

O marco de controle que a MASISA projetou para resguardar todos seus ativos de informação são as POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO, as quais deverão ser aplicadas por todos os funcionários da MASISA dentro de suas atividades e competências.

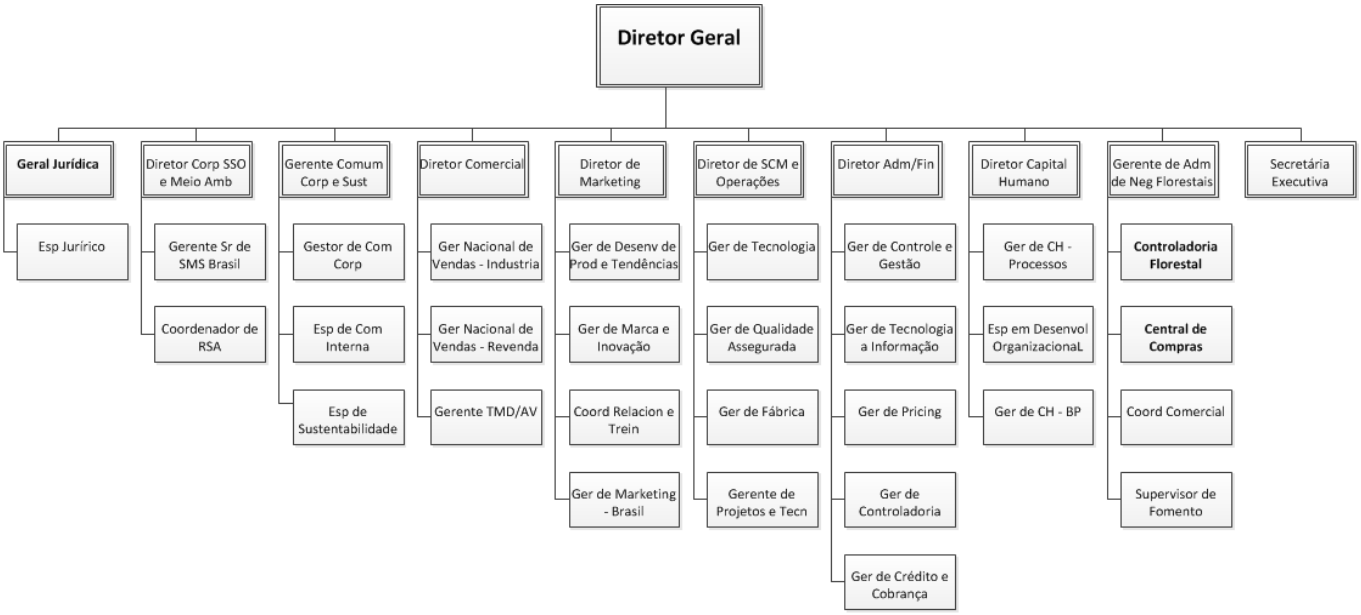


Figura 12 – Organograma da Gestão Corporativa Masisa do Brasil
Fonte: Portal Interno Masisa

A Masisa é uma empresa Chilena no ramo da madeira, com sua sede em Santiago e possui presença em mais 9 paises da América Latina. Mas nosso foco do trabalho será apenas o Brasil. Onde produz MDF na unidade de Ponta Grossa - PR e MDP em Montenegro - RS. Possui duas sedes administrativas em Curitiba e São Paulo, juntamente com os centro de distribuições que utilizam nossa VPN e SAP. Trabalha ainda com alguns serviços compartilhados (entre elas a TI), com a empresa Louisiana Pacific, que comprou a linha de OSB da unidade de Ponta Grossa e possui sua sede administrativa a duas quadras dos escritório da Masisa de Curitiba, também assistida pelo nosso suporte.

3.2 INFRAESTRUTURA FÍSICA

A segurança física é mantida por uma equipe formada por profissionais relacionados à Segurança Patrimonial.

A segurança física/patrimonial da Masisa do Brasil contempla os seguintes ativos:

TOPOLOGIA

Mapa da Estrutura de rede a nivel de Brasil (Ponta Grossa - PR, Montenegro - RS, Curitiba - PR, São Paulo - SP e outros pontos móveis dos Centros de Distribuição)

Não se é utilizadas VLANs internas, todos os equipamentos (sendo PCs, Impressoras, Switchs, Servidores) se enchergam entre si entre todas as unidades do Brasil.

Serviços Suportados:

pontos sobrecarregados com Hubs

falta de nova identificação dos pontos de acesso do cliente com os racks centrais

Permissões de administrador local desnecessariamente para os usuarios, não tendo o controle efetivo das instalações e programas piratas feitos diretamente por esses usuarios.

Acesso irrestrito (sem rede guest, enchergando todas as maquinas internas e mesma faixa de IP) para qualquer usuario que conectar via cabo LAN, para qualquer computador de 3° e auditores externos.

Grande parte dos servidores foram virtualizados via VMware.

FILE SERVER

Pastas do File Server sem um proprietário principal, necessitando de um reinventário das permissões

Criação e Organização de Grupos Leitura e Escrita.

procedimentos de BACKUP: Full - Mensal e Semanal, Diferencial - Diário:

Em PGO e MON - O Backup é armazenado na Portaria a mais de 500m do File Server.

Em CWB - Backup é temporariamente salvo (somente mensal), no Escritório da Empresa LP, a duas quadras do prédio da Masisa (Porém, como estamos em transição de separação entre as empresas, tem de se encontrar outra solução para o armazenamento fora do prédio)

Em SPO o Serviço de File Server, é feito do mesmo procedimento de PGO e MON. Porém, com o backup armazenado no mesmo local.

Existe regras de bloqueio quanto a videos, musicas e imagens.

VOIP

Em Ponta Grossa os VOIPs são da Siemens e a central telefonica é na próprio unidade e administrados pela equipe local. (30 aparelhos)

Em SPO (27 aparelhos), CWB e MON(ainda sem essa informação de qtde e faixa de IP), são VOIPs da Cisco, a central é no Chile e administrado pelos mesmos.

PABX

Hicom 300 Na Masisa Ponta Grossa, gestionando 300 ramais

Hicom 150 Na LP Curitiba, gestionando 20 ramais

3.2.1 Planta Ponta Grossa

- Portaria: 2 catracas para controle de acesso de pessoas; 3 seguranças terceirizados da empresa Prosegur, 1 porteiro para controles de entrada e saída de pessoal;
- Estacionamentos: 1 externo para terceiros, 1 estacionamento para funcionários diretos e 1 para supervisores, coordenadores, gerencia e diretoria; 2 cancelas, sendo compartilhada com o fluxo de caminhões de carga e descarga; registro de controle somente para pedestres na lateral;
- CPD: controle de acesso via cartão magnético de identificação do funcionário (crachá). Liberado somente aos responsáveis pela segurança da informação.
- Estações de trabalho devidamente controladas e identificadas.
- Grande parte dos servidores estão virtualizados via VMware.

3.2.2 Sistema de CFTV Logistica e Melamina;

Segurança patrimonial: sistema de leitor de crachás para acesso a áreas controladas/restritas, tais como: Almoxarifado e CPD;

Portal Masisa: Local vinculado ao email corporativo, onde estão contidas as notícias internas da Masisa, sua visão e missão, bem como todas as políticas, procedimentos e regras da empresa;

3.3 INFRAESTRUTURA TECNOLÓGICA

- **Situação atual de Segurança da Informação na empresa no Brasil.**

Subordinada a área de TI, a área de Segurança da Informação conta com um profissional que atua na função de Supervisor da área de Tecnologia, sendo responsável pela elaboração e gerenciamento de políticas e práticas de segurança. Trabalha em conjunto com o pessoal de TI de cada unidade e também executa periodicamente auditorias internas, além de trabalhos de conscientização junto aos funcionários. O poder de decisão deste profissional está subordinado ao gerente de TI.

A área de TI Masisa Brasil encontra-se atualmente subordinada ao diretor financeiro enquanto país e responde ao Chile a nível coorporativo.

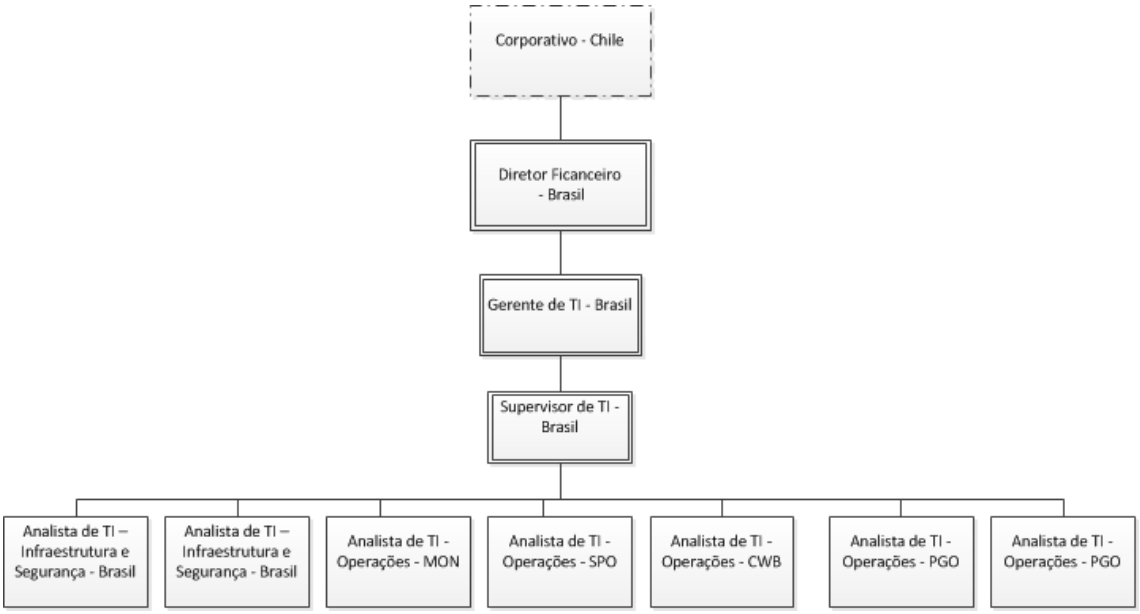


Figura 13 – Organograma da Gestão de TI Masisa do Brasil
Fonte: Portal Interno Masisa

3.3.1 Ativos de tecnologia

A estrutura suportada pela área de TI da Masisa atualmente é composta por:

Tabela 9 – Inventário Masisa Brasil

Local	Ativo	Valor contábil
Ponta Grossa	Desktop	R$ 165.354,15
	Notebook	R$ 149.529,01
	Servidores	R$ 4.371,25
	Impressoras	R$ 63.828,30
	Outros	R$ 168.672,40
	TOTAL	R$ 551.755,11

Local	Ativo	Valor contábil
Curitiba	Desktop	R$ 44.183,14
	Notebook	R$ 137.113,83
	Servidores	R$ 73.521,57
	Impressoras	R$ 14.160,49
	Outros	R$ 110.462,28
	TOTAL	R$ 379.441,31

Local	Ativo	Valor contábil
Montenegro	Desktop	R$ 59.786,16
	Notebook	R$ 130.557,29
	Servidores	R$ 37.691,74
	Impressoras	R$ 36.083,03
	Outros	R$ 158.953,87
	TOTAL	R$ 423.072,09

Local	Ativo	Valor contábil
São Paulo	Desktop	R$ 19.030,99
	Notebook	R$ 417.200,13
	Servidores	R$ 63.005,41
	Impressoras	R$ 5.696,46
	Outros	R$ 117.597,46
	TOTAL	R$ 622.530,45

Local	Ativo	Valor contábil	Valor contábil
BRASIL	Desktop	340	R$ 288.354,44
	Notebook	273	R$ 834.400,26
	Servidores	50	R$ 178.589,97
	Impressoras	166	R$ 119.768,28
	Outros		R$ 555.686,01
	TOTAL		R$ 1.976.798,96

Fonte: Desenvolvido pelo autor

3.3.2 Serviços

Tabela 10 – Serviços executados na Masisa Brasil

Localidade	Software	Sistema
Ponta Grossa	Guardian	Pesagem caminhões e vagões
	RONDA	sistema de controle de acesso
	START	Tarifador
	JOINRH	Sistema de organograma/plano de carrega/pesquisa salarial
	Forponto	Relatórios de RH
	Hipath 3000	Gerenciamento da Central Telefonica
	Faxination	Faxination
	Sislab	Controle Laboratorio
	Sisdoc	Controle documentos Engenharia
	SAPSprint	Etiquetas SAP
	ISA Server	Proxy
	Symantec	Console Anti virus
	SAPSprint	Notas Fiscais SAP
	Sinteg	Sistema de controle de produção via plc
	Symantec	Console Antivirus
	Solide	Base antiga dos cartões ponto
Curitiba	TECWIn	Sistema Aduaneiro - Tarifa Externa Comum
	PGRTCP	Sistema Coleta de Marcações
	START	Tarifador
	Symantec	Console Anti virus
	ISA Server	Proxy
	WebSense	Filtro Conteudo - WebSense
Montenegro	Guardian	Pesagem caminhões e vagões
	Forponto	Controle Ponto
	Foracesso	Controle Acesso

Fonte: Desenvolvido pelo autor

3.3.3 Topologia Lógica da Rede

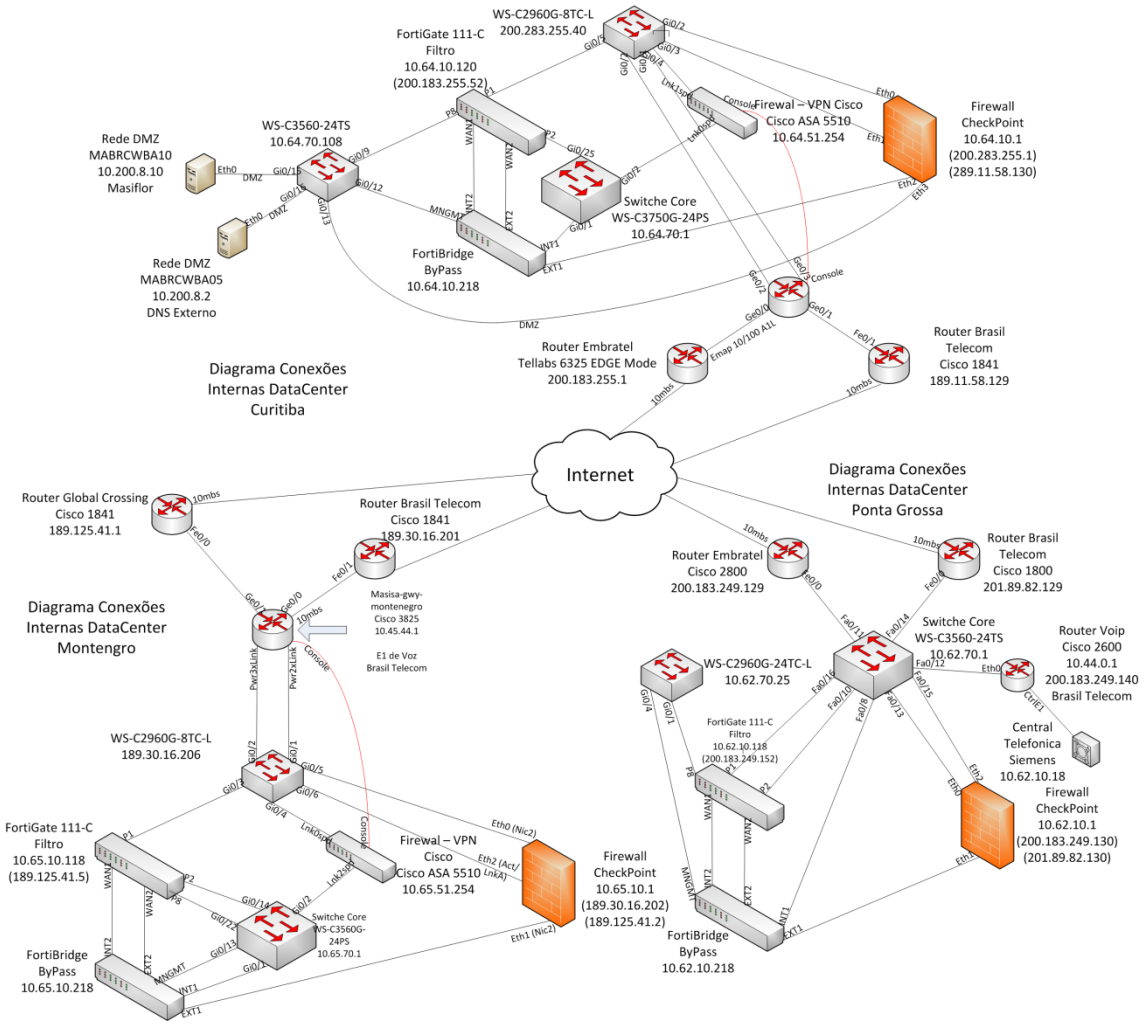


Figura 14 – Diagrama de Conexões Internas Data Center Masisa Brasil
Fonte: Documentação Interna

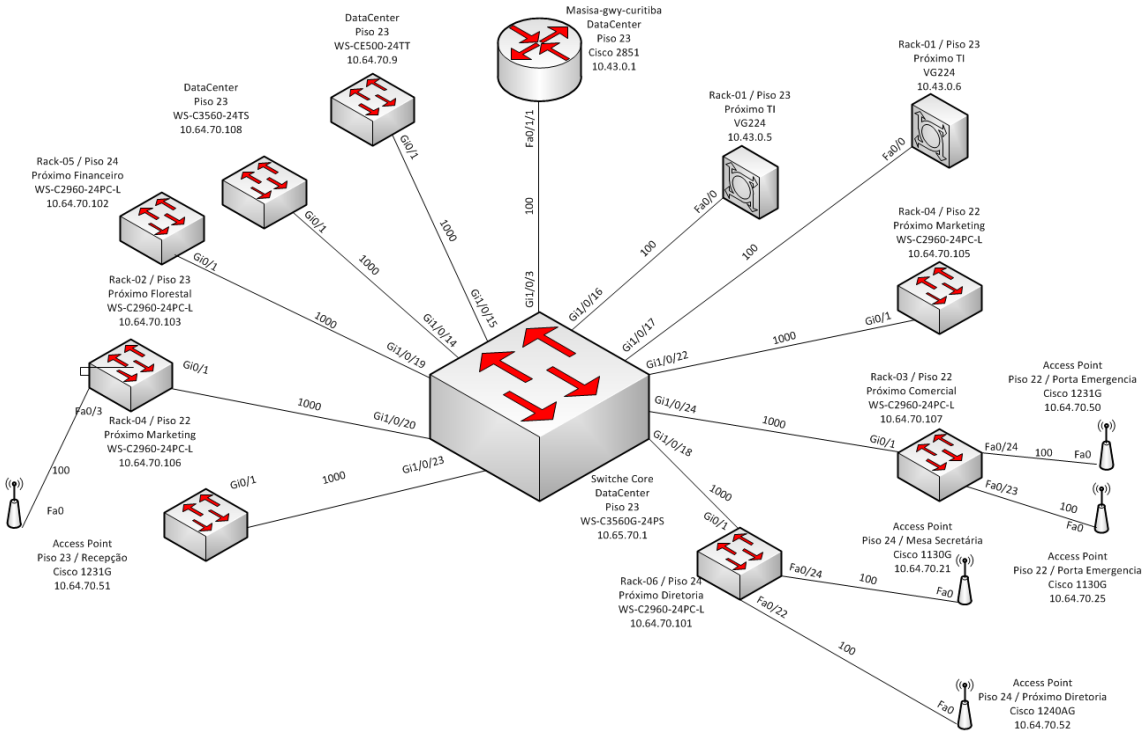


Figura 15 – Topologia Interna da Rede de Curitiba
Fonte: Documentação Interna

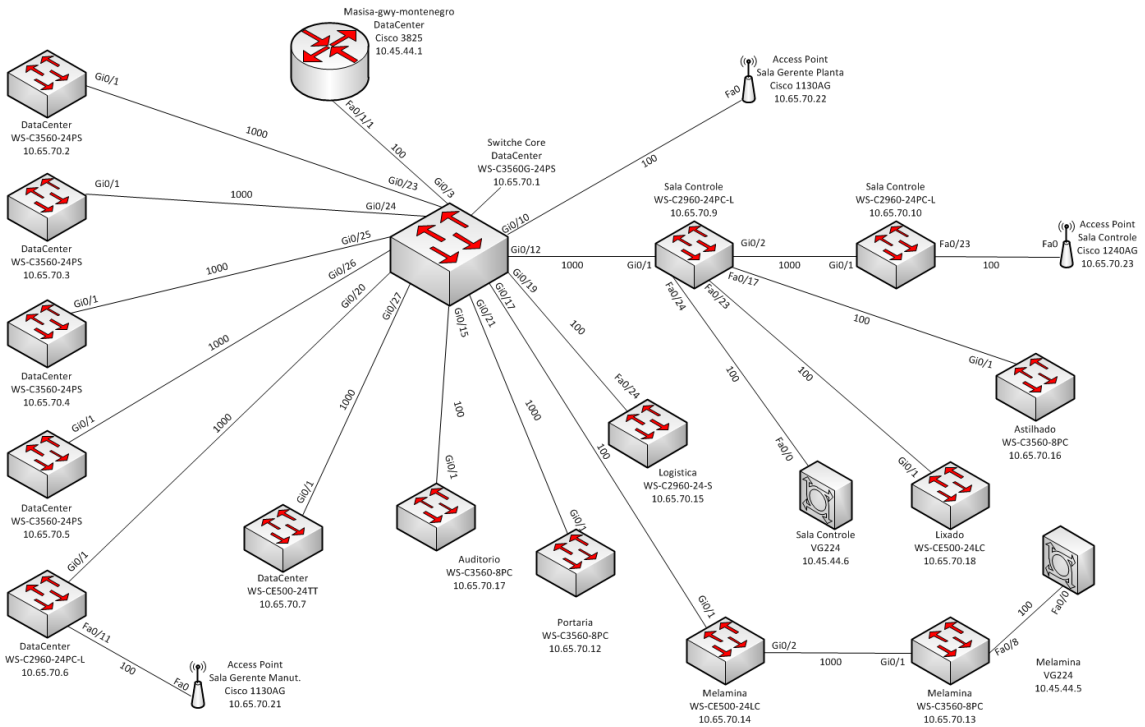


Figura 16 – Topologia Interna da Rede de Montenegro
Fonte: Documentação Interna

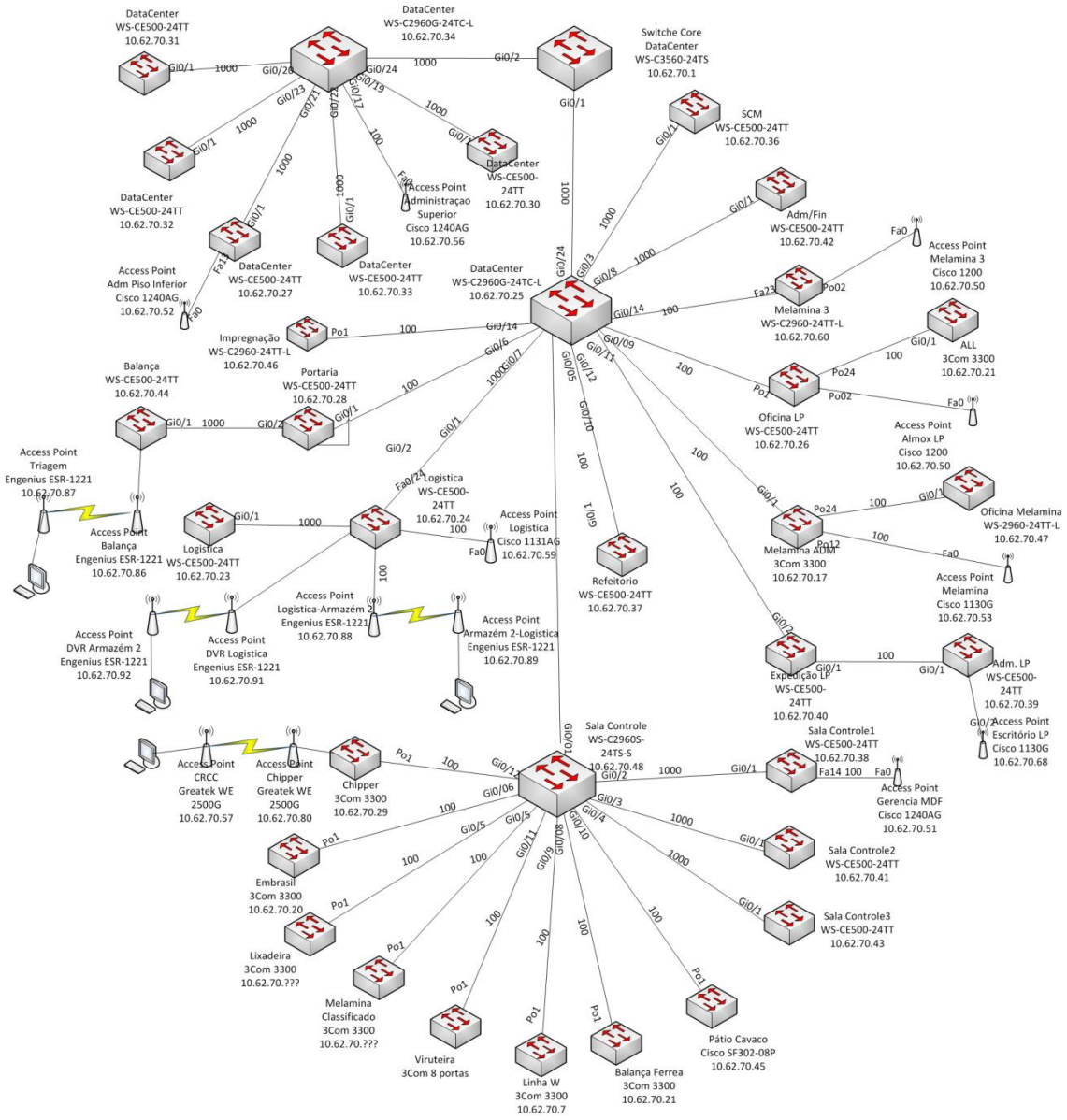


Figura 17 – Topologia Interna da Rede de Ponta Grossa
Fonte: Documentação Interna

3.3.4 Telecomunicações

Tabela 11 – Inventário dos serviços de telecomunicação da Masisa Brasil

Operadora	Modelo	Qtde
TIM	Blackberry	4
	Android	73
	IPhone	7
	Celular Tim	130
	Tim Web	10
	CELFs	18
VIVO	Celular Vivo	10
	Vivo ZAP	130
OI	Celular Oi	2

Rede	VOIPs	362
PABX	Analógicos/Digitais	190

Fonte: Desenvolvido pelo autor

3.4 MÉTODO ISHIKAWA

Envolve toda estrutura pertinente ao tráfego da rede, tais como: roteadores, switchs, pontos de rede, racks, conversores de fibra, fibra optica, antenas via radio, access points.

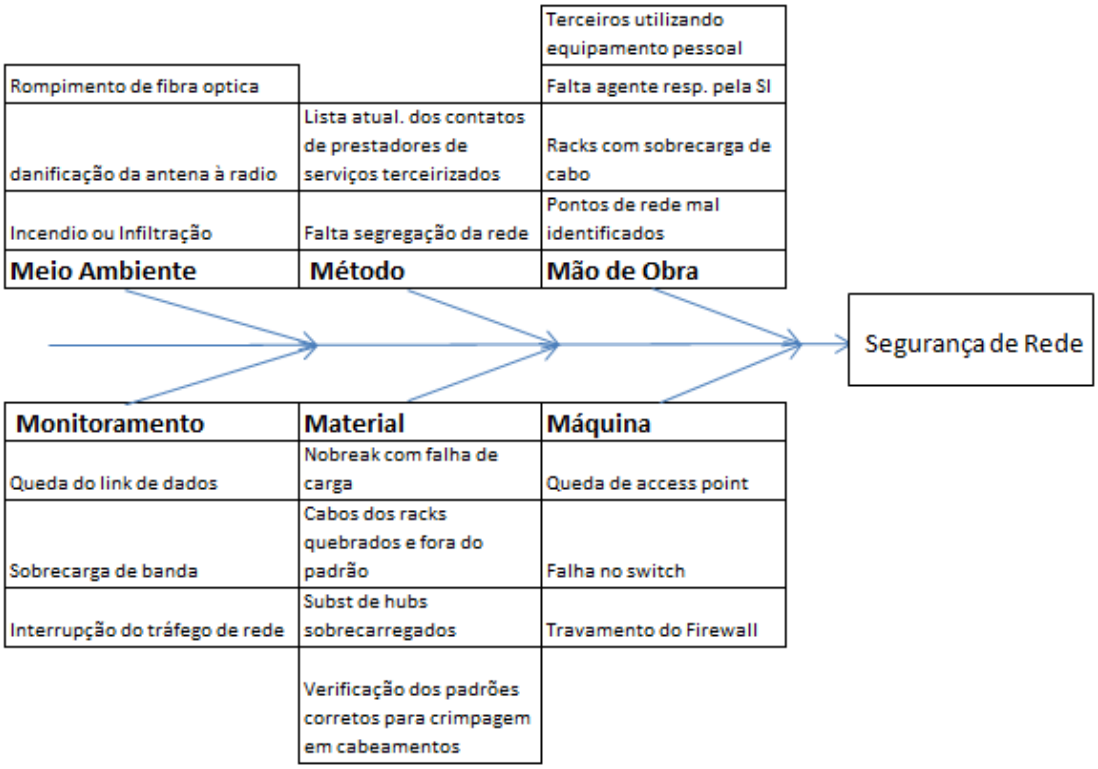


Figura 18 – Diagrama de Ishikawa para segurança de rede
Fonte: Desenvolvido pelo autor

Envolve todos os equipamentos de hardware e a própria informação em forma de dados: notebooks, desktops, impressoras, monitores.

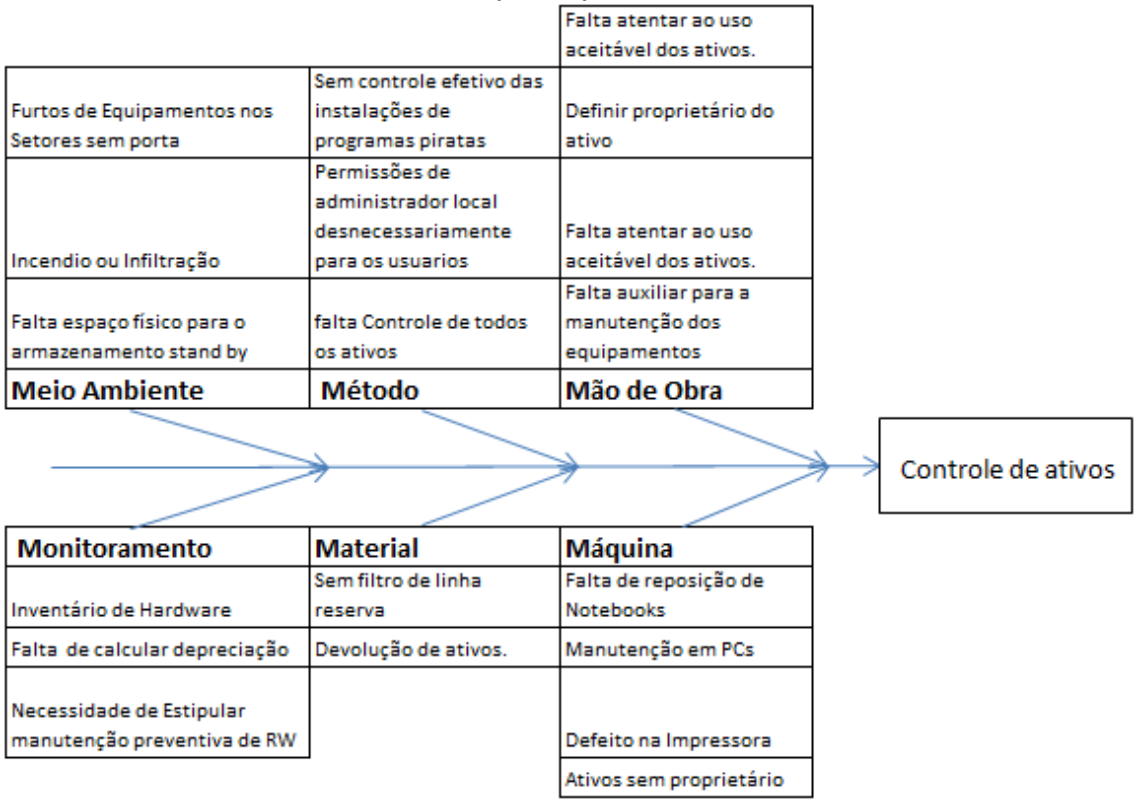


Figura 19 – Diagrama de Ishikawa para controle de ativos
Fonte: Desenvolvido pelo autor

Envolve toda a area física das plantas e escritórios

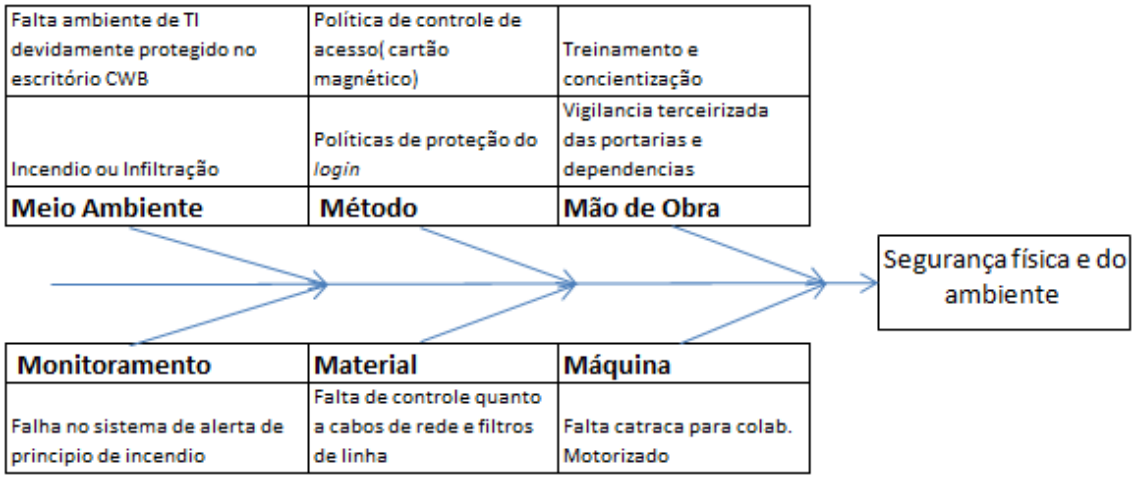


Figura 20 – Diagrama de Ishikawa para segurança física e do ambiente
Fonte: Desenvolvido pelo autor

Envolve todos os serviços suportes pelos servidores centralizados no CPD: Tais como, SAP, WSUS, Antivirus, Serv de arquivos.

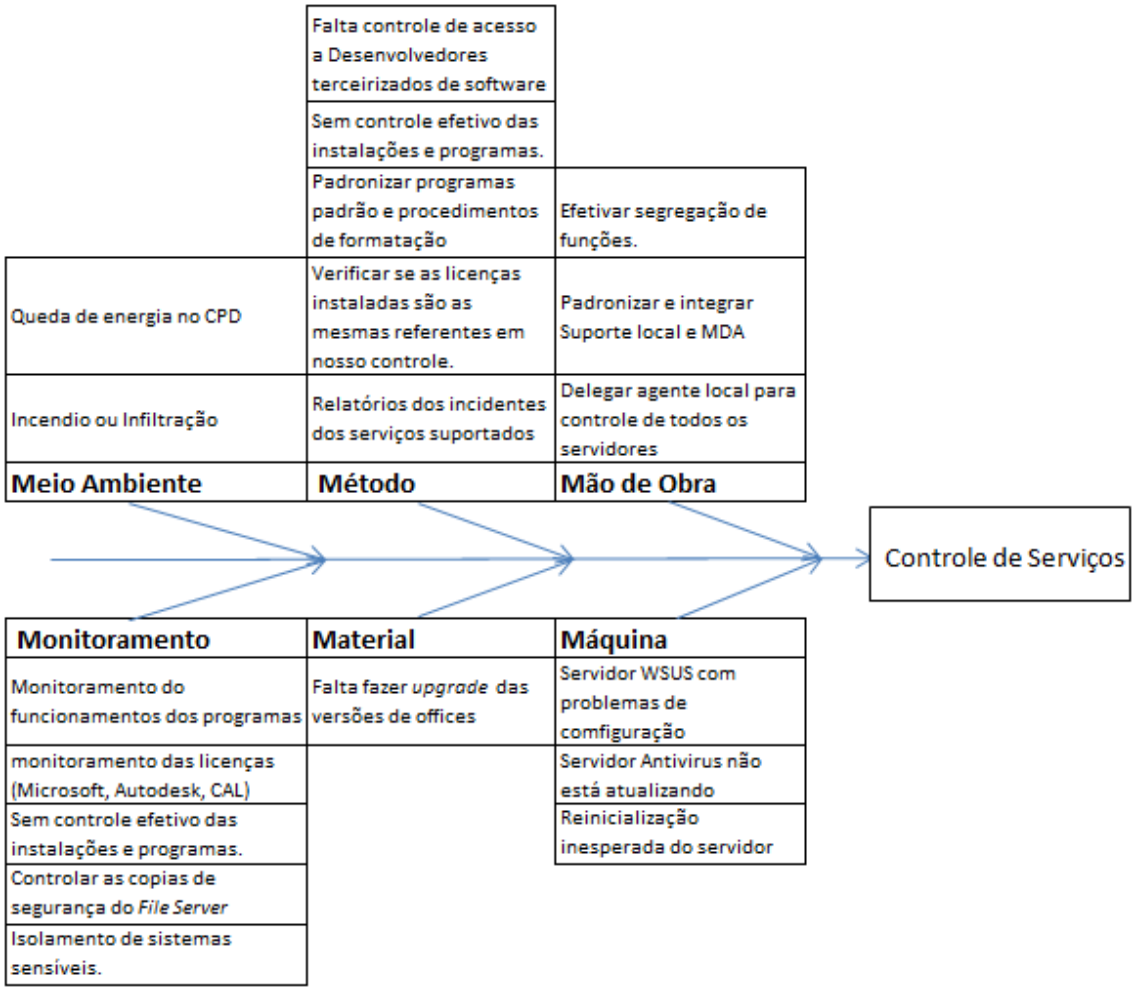


Figura 21 – Diagrama de Ishikawa para controle de serviços
Fonte: Desenvolvido pelo autor

Envolve todos os serviços de telefonia e links de comunicação

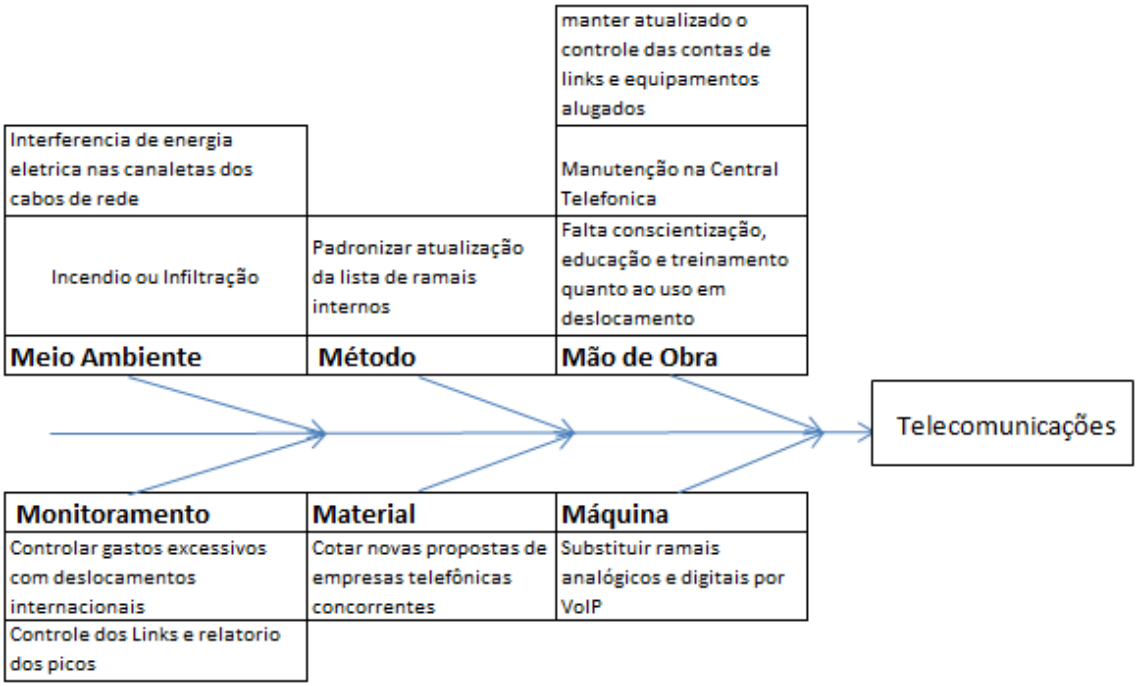


Figura 18 – Diagrama de Ishikawa para telecomunicações
Fonte: Desenvolvido pelo autor

3.6 MÉTODO MARAT

Definido 5 macrofatores e 5 principais ameaças que podem vir a ser tornar um risco a MASISA:

Tabela 12 – Matriz de Probabilidade e Impacto

	MATRIZ DE PROBABILIDADE E IMPACTO		ND	NE	NP=(NDxNE)	NS	NR=(NPxNS)
1	Segurança da Rede	Rompimento de fibra optica de um setor	2 - Insuficiente	1 - Esporática	2 - Muito Baixa	60 - Moderado	120
2	Segurança dos Ativos	Furtos de Equipamentos nos Setores sem porta	6 - Deficiente	2 - Pouco Frequente	12 - Média	25 - Leve	300
3	Segurança Física e do Amb	Incendio no CPD	1 - Aceitável	1 - Esporática	1 - Muito Baixa	155 - Catastrófico	155
4	Segurança dos Serviços	Servidor Antivirus não está atualizando	6 - Deficiente	3 - Ocasional	18 - Média	25 - Leve	450
5	Telecomunicações	Queda de energia no CPD	2 - Insuficiente	2 - Pouco Frequente	4 - Baixa	155 - Catastrófico	620

Fonte: Desenvolvido pelo autor

A medição do Nível de Risco, com base na tabela acima, levantou o seguinte diagnóstico:

1) ROMPIMENTO DE FIBRA ÓPTICA DE UM SETOR

Nível de Severidade: Requer parada das atividades para efetuar a reparação. Não há danos pessoais.
Nível de Probabilidade: Não é de esperar que o risco se materialize.
Nível de Intervenção: IV – Melhorar se possível justificando a intervenção.
Nível de aceitabilidade: Aceitável.

2) FURTOS DE EQUIPAMENTOS NOS SETORES SEM PORTA

Nível de Severidade: Reparação sem parada das atividades. Não há danos pessoais.
Nível de Probabilidade: A materialização do risco é passível de ocorrer.
Nível de Intervenção: IV – Melhorar se possível justificando a intervenção.
Nível de aceitabilidade: Aceitável.

3) INCENDIO NO CPD

Nível de Severidade: Destruição de um ou mais sistemas (difícil renovação / reparação). Lesões graves que poder ser irreparáveis.
Nível de Probabilidade: Não é de esperar que o risco se materialize.
Nível de Intervenção: IV – Melhorar se possível justificando a intervenção.
Nível de aceitabilidade: Aceitável.

4) SERVIDOR ANTIVIRUS NÃO ESTÁ ATUALIZANDO

Nível de Severidade: Reparação sem parada das atividades. Não há danos pessoais.
Nível de Probabilidade: A materialização do risco é passível de ocorrer.
Nível de Intervenção: III – Situação a melhorar. Deverão ser elaborados planos, programas ou procedimentos documentos de intervenção.
Nível de aceitabilidade: Inaceitável.

5) QUEDA DE ENERGIA NO CPD

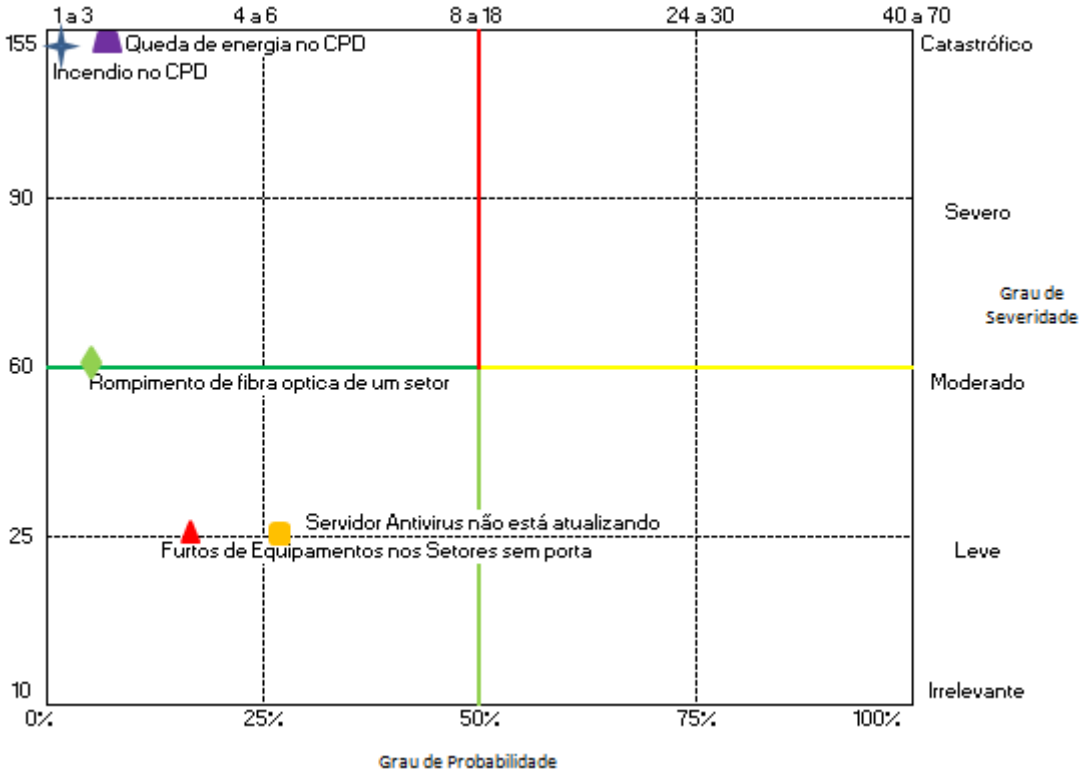
Nível de Severidade: Destruição de um ou mais sistemas (difícil renovação / reparação). Não há danos pessoais.
Nível de Probabilidade: A materialização do risco pode ocorrer.
Nível de Intervenção: III – Situação a melhorar. Deverá ser elaborados planos, programas ou procedimentos documentos de intervenção.
Nível de aceitabilidade: Inaceitável.

Tabela 13 – Matriz de Probabilidade e Severidade

Simb	MATRIZ DE PROBABILIDADE E SEVERIDADE		NP	NS	Níve de Impacto
	1 Seg da Rede	Rompimento de fibra optica de um setor	3%	60	Moderado
	2 Seg dos Ativos	Furtos de Equip nos setores s/ porta	17%	25	Leve
	3 Seg física e do ambiente	Incendio no CPD	1%	155	Catastrófico
	4 Seg dos Serviços	Servidor Antivirus não está atualizando	26%	25	Leve
	5 Telecomunicações	Queda de energia no CPD	6%	155	Catastrófico

Fonte: Desenvolvido pelo autor

Tabela 14 – Gráfico da avaliação dos riscos



Fonte: Desenvolvido pelo autor

4 CONSIDERAÇÔES FINAIS

Este estudo atingiu os objetivos estabelecidos, que era colaborar como um instrumento de reconhecimento a respeito da importância da segurança da informação. A maioria dos incidentes envolvendo a segurança da informação está diretamente ligada ao fator humano. Sendo assim, os investimentos não terão o retorno esperado se a conscientização de todos os envolvidos.

REFERÊNCIAS

FONTES, Edison Luiz G. **Políticas e Normas Para A Segurança Da Informação.** Rio de Janeiro: Editora Brasport, 2011

MATOS, Francisco Marcelo A. **Proposta de um Checklist Para Verificação Da Segurança Física De Uma Empresa Baseada Na Norma ABNT NBR ISO/IEC 27002:2005.** Fortaleza: Campus, 2010

WADLOW, Thomas. **Segurança de Redes.** Rio de Janeiro: Campus, 2000

LIMA, Guilherme. **Segurança da Informação em Windows Server 2008.** Disponível em <HTTP://www.slideshare.net/khaotikuz/segurana-da-informao-com-windows-server> Acesso em 08/08/13, 20:00

ALVES, Cássio Bastos. **Segurança da Informação VS. Engenharia Social.** Como se Proteger para não ser mais uma Vítima. Brasília: Campus, 2010

PEIXOTO, Mário C.P. **Engenharia do Social E Segurança Da Informação Na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006

COELHO, Cláudia Sanches. RIBEIRO, Daniele Aparecida da Silva. FERREIRA, Kelson. **Governança Corporativa.** Marília: Campus, 2010

COUTINHO, Ítalo de Azevedo. **Estudo da Aderência dos Processos de Gestão de Projetos em Empresas de Engenharia.** Consultiva de Belo Horizonte. Belo Horizonte: Campus, 2009

HORI, Andre Shigueru. **Modelo de Gestão de Risco em Segurança da Informação:** um Estudo de Caso no Mercado Brasileiro de Cartões de Crédito. São Paulo: Campus, 2003

MARQUES, Vítor. **Modelos de Avaliação de Riscos.** O MARAT. 2º ed. Disponível em < www.forma-te.com/mediateca/download-document/modelos-de-avaliacao-de-riscos.html > Acesso em 06/09/13, 22:40

SELLA, Danilo. **Segurança da Informação.** Um Diferencial Determinante Na Competitividade Das Corporações. Promon Business & Technology Review**:** São Paulo, 2005

SILVEIRA, Andrey. **Auditoria de Sistemas – Proposta de Solução para Gerenciamento e Controle de Auditorias.** Novo Hamburgo: 2009

APÊNDICE A - POLÍTICA DE SEGURANÇA E PROTEÇÃO DA INFORMAÇÃO

Documento baseado em Regulamentos Exemplos de Edison Fontes, 2012.

1. OBJETIVO

Definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia da MASISA.
As orientações aqui apresentadas são os princípios fundamentais e representam como a MASISA exige que a informação seja utilizada.

2. ABRANGÊNCIA

Esta política se aplica:
A todos os usuários (associados, prestadores de serviços e estagiários) que utilizam as informações da MASISA;
A todas as organizações que compõem o Grupo MASISA.

3. IMPLANTAÇÃO

A Gerência de Segurança da Informação coordenará as áreas técnicas, as áreas de apoio e as áreas de negócio para desenvolvimento e implantação de projetos, procedimentos, ações, instruções e normativos que possibilitem a operacionalização e manutenção desta política.

4. DIRETRIZES E REGRAS

4.1 – O bem informação

A informação utilizada pela MASISA é um bem que tem valor. A informação deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

4.2 – O Gestor da Informação (GI)

a) Cada informação deverá ter o seu Gestor que será indicado formalmente pela diretoria responsável pelos sistemas que acessam a informação.
b) O Gestor da Informação é a pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação.

4.3 – Confidencialidade da informação

a) O Gestor da Informação classificará o nível de confidencialidade e sigilo da informação baseando-se nos critérios estabelecidos na Norma de Classificação da Informação.
b) A confidencialidade da informação deve ser mantida durante todo o processo de uso da informação e pode ter níveis diferentes ao longo da vida dessa informação.

4.4 – Utilização da informação e recursos

A liberação do acesso da informação para os usuários será autorizada pelo Gestor da Informação, que considerará a necessidade de acesso do usuário e o sigilo da informação para a realização dos objetivos da MASISA.

O acesso da informação deve ser autorizado apenas para os usuários que necessitam da mesma para o desempenho das suas atividades profissionais para a MASISA.

Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso consciente a ambientes não autorizados será considerada uma falta grave.

O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Este acesso acontece através da identificação e da autenticação do usuário. Os dados para a autenticação do usuário devem ser mantidos em segredo e possuem o mais alto nível de classificação da informação.

Os recursos de tecnologia da MASISA disponibilizados para os usuários têm como objetivo a realização de atividades profissionais. A utilização dos recursos da MASISA com finalidade pessoal é permitida, desde que seja em um nível mínimo e que não viole a Política de Segurança e Proteção da Informação e o Código de Conduta e Ética da MASISA.

4.5 – Proteção da informação

Toda informação da MASISA deve ser protegida para que não seja alterada, acessada e destruída indevidamente.

Os locais onde se encontram os recursos de informação devem ter proteção e controle de acesso físico compatível com o seu nível de criticidade.

4.6 – Continuidade do uso da informação

Toda informação utilizada para o funcionamento da MASISA deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção equivalente ao local principal. Esta informação deve ser suficiente para a existência de planos de continuidade de negócio.

A criação das cópias de segurança deve considerar os aspectos legais, históricos, de auditoria e de recuperação do ambiente.

Os recursos tecnológicos, de infraestrutura e os ambientes físicos onde são realizadas as atividades operacionais do negócio da MASISA devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade de negócio.

A definição e implementação das medidas de prevenção e recuperação, para situações de desastre e contingência, devem ser efetuadas de forma

permanente e devem contemplar recursos de tecnologia, humanos e de infraestrutura. Elas são de responsabilidade da diretoria gestora dos recursos, contando com o apoio e validação da Gerência de Segurança da Informação.

4.7 – Computação pessoal e móvel

As informações estruturadas e sistemas da MASISA somente serão utilizados em recursos da MASISA. É proibido o uso de equipamentos pessoais para acessar informações estruturadas e sistemas corporativos da MASISA.

4.8 – Correio Eletrônico

As mensagens do correio eletrônico disponibilizado para os usuários obrigatoriamente devem ser escritas em linguagem profissional e que não comprometa a imagem da MASISA, não vá de encontro à legislação vigente e nem aos princípios éticos da MASISA. Cada usuário é responsável pela conta de correio eletrônico que lhe foi disponibilizada pela MASISA.

O conteúdo do correio eletrônico de cada usuário pode ser acessado e monitorado pela MASISA quando em situações que ponham em risco a sua imagem, seu negócio ou sua lucratividade. O usuário não deve ter expectativa de sigilo da sua conta de correio eletrônico disponibilizada pela MASISA para seu uso profissional.

4.9 – Ambiente de Internet

O ambiente de Internet deve ser usado para o desempenho das atividades profissionais do usuário para a MASISA. *Sites* que não contenham informações que agreguem conhecimento profissional e para o negócio não devem ser acessados. Os acessos realizados nesse ambiente são monitorados pela MASISA com o objetivo de garantir o cumprimento dessa política.

4.10 – Redes Sociais

Os usuários obrigatoriamente devem seguir as regras de uso de Serviços de Rede Social descritos na norma específica.

4.11 – Documentação

Todos os procedimentos que possibilitam a proteção da informação e a continuidade do seu uso devem ser documentados, de tal forma que possibilite que a MASISA continue a operacionalização desses procedimentos, mesmo na ausência do usuário responsável.

5. CONCLUSÃO

A segurança e proteção da informação é uma responsabilidade contínua de cada usuário da MASISA em relação às informações que acessa e gerencia. Todos os usuários devem utilizar a informação da MASISA, de acordo com as determinações desta Política de Segurança e Proteção da Informação. O não cumprimento desta política e/ou dos demais instrumentos normativos que

complementarão o processo de segurança constitui em falta grave, e o usuário está sujeito a penalidades administrativas e/ou contratuais.