CENTRO UNIVERSITÁRIO UNIVESC
CIÊNCIAS DA COMPUTAÇÃO
TRABALHO DE CONCLUSÃO DE CURSO

CHECKLIST PARA ANÁLISE DA POLÍTICA DA INFORMAÇÃO DOS SUPERMERCADOS MYATÃ LTDA COM BASE NA NORMA ABNT NBR ISO/IEC 27002:2005

Área: Segurança da informação

GREGORY BORBA RAMOS

LAGES (SC), AGOSTO DE 2012.

CENTRO UNIVERSITÁRIO UNIVESC
CIÊNCIAS DA COMPUTAÇÃO
TRABALHO DE CONCLUSÃO DE CURSO

CHECKLIST PARA ANÁLISE DA POLÍTICA DA INFORMAÇÃO DOS SUPERMERCADOS MYATÃ LTDA COM BASE NA NORMA ABNT NBR ISO/IEC 27002:2005

Área: Segurança da informação

GREGORY BORBA RAMOS

Monografia apresentada como exigência para obtenção do grau de Bacharelado em Ciências da Computação do Centro Universitário Univesc.

LAGES (SC), AGOSTO DE 2012.

EQUIPE TÉCNICA

Acadêmico
Gregory Borba Ramos

Professor Orientador
Profº. Marcio José Sembay, Msc.

Coordenador de TCC
Profº. Marcio José Sembay, Msc.

Coordenador do curso
Profº. Marcio José Sembay, Msc.

SUMÁRIO

RESUMO

Este trabalho tem como finalidade a análise da conformidade da segurança da informação de uma empresa do varejo com a aplicação de um *checklist* desenvolvido com base nos requisitos de segurança da norma ABNT NBR ISO/IEC 27002:2005. O uso cada vez mais disseminado de sistemas informatizados integrados fez com que a informação se tornasse o ativo mais importante das empresas e protegê-la das ameaças constantes é um processo difícil e demorado. Atualmente não existe um meio que possa ser comprado e resolva todos os problemas instantaneamente. Para se alcançar um nível aceitável de segurança é necessário um processo de avaliação e tomada de decisões constantes.

Palavras-chave: Conformidade, *Checklist*, Segurança da informação, ABNT NBR ISO/IEC 27002:2005.

ABSTRACT

This paper aims at analyzing the compliance of information security from a retail company with the application of a *checklist* developed based on the security requirements of the standard ABNT NBR ISO/IEC 27002:2005. The increasingly widespread use of integrated information systems meant that the information could become the most important asset of enterprises and protect it from the constant threats is a difficult and lengthy process. Currently there is no way that can be purchased and solve all the problems instantly. To achieve an acceptable level of security is needed is a process of evaluation and decision making constant.

Keywords: Compliance, *Checklist*, Information Security, ABNT NBR ISO/IEC 27002:2005.

AGRADECIMENTOS

Agradeço ao dia em que meus pais resolveram ficar juntos e proporcionar a chance de chegar ate aqui, o apoio e dedicação com que fui criado e as intermináveis horas de broncas e permissões negadas.

Agradeço ao tempo que dediquei jogando vídeo game, pois graça a ele nunca esquecerei o quanto minha infância foi divertida.

Agradeço a minha irmã por ser a garotinha maravilhosa que é.

Agradeço aos meus amigos que chegaram até a este momento, os que não chegaram também, que sempre estavam ao meu lado na hora de reclamar de alguma coisa, rindo muito nas longas conversas e atravessando os obstáculos da faculdade.

Agradeço a burocracia e dificuldade que é fazer alguma coisa na faculdade que faz com que se valorize cada vez mais este momento.

Agradeço aos professores que se dedicaram a transmitir seus conhecimentos e aos professores que tentaram e não conseguiram transmiti-los.

E por fim agradeço a Deus por me dar a oportunidade, vontade e força de chegar até aqui.

LISTA DE ABREVIATURAS

ABNT – Associação Brasileira de Normas e Técnicas

CPD – Centro de Processamento de Dados

DNS – *Domain name System*

ID – Identificação Digital

IEC – *International Electrotechnical Commission*

IP – *Internet Protocol*

ISO – International Organization for Standardization

LTDA – Limitada

NBR – Norma Brasileira

PIN – *Personal Identification Number*

SO – Sistema Operacional

TCC – Trabalho de Conclusão de Curso

TCP – *Transmission Control Protocol*

LISTA DE TABELAS

INTRODUÇÃO

O uso cada vez maior de sistemas integrados e o advento das redes mundialmente interligadas fez com que a informação se tornasse o ativo mais importante da organização. O bem mais valioso de uma empresa pode não ser produzido pela linha de produção ou serviços prestados, mas as informações relacionadas com esse bem de consumo ou serviço. É importante que os executivos em geral se conscientizarem que todas as informações tem algum tipo de valor para alguém ou algo. (Caruso e Steffen, 1999).

Com essa preocupação em torno das informações que são trocadas durante a comunicação e transações dentro e fora da organização surgiu a segurança da informação com objetivo de regularizar a forma como os dados serão protegidos e reduzir os impactos dos incidentes que podem vir a acontecer. A informação corre riscos em todo o seu ciclo de vida, desde sua criação ate o descarte de forma adequada.

Uma política de segurança que traga a informação um nível aceitável de riscos é um processo lento, caro e delicado, pois, toda a organização deve ser levada em consideração, suas características e passos envolvidos nos planos de negócio.

O desenvolvimento de uma política de segurança da informação visa estabelecer regras baseadas em normas para que as informações importantes da empresa tenham a proteção necessária para garantir a sua integridade, confidencialidade e disponibilidade abrangendo desde a segurança física das instalações ate normas legais de continuidade dos planos de negócio.

Nesse sentido esta monografia consiste em um *checklist* para verificação da conformidade da política de segurança dos supermercados Myatã LTDA com a norma ABNT NBR ISO/IEC 27002:2005. Esta norma estabelece diretrizes e princípios gerais para a construção e manutenção de uma gestão de segurança da informação. O objetivo é ser utilizada como um guia prático para desenvolver uma política de segurança abrangente a todos os setores e processos de negócio da organização.

1.1 Justificativa

Atualmente a informática tem uma grande importância dentro das organizações. Graças às redes de computadores e a internet a velocidade que a informação se propaga é imensa e vem aumentando a cada dia. A informática tornou-se essencial para a realização dos

processos administrativos, a segurança no mundo das redes vem ganhando importância, as informações que os usuários acessam precisam ser confiáveis, integras e sempre estarem disponíveis. (Geus, Nakamura, 2003).

Na sociedade a informação é o principal patrimônio da empresa e esta sob constante risco. A informação é o substrato da inteligência competitiva, deve ser administrada em suas particularidades, diferenciada e salvaguardada. (Dias, 2000).

Segurança é a base para as empresas tenham a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócio, a não aplicação de uma boa política de segurança da informação pode desencadear em invasões no sistema, perda e danos em suas informações mais relevantes, podendo acontecer de seus processos de negócio sofrerem danos irreparáveis. (Widlow, 2004).

1.2 Importância

A informação é o dado com uma interpretação lógica ou natural dada a ele por seu usuário (Rezende e Abreu, 2012). A informação tem um valor altamente significativo e pode representar grande poder para quem a possui, ela contém valor, pois está integrada com os processos, pessoas e tecnologias.

Para Geus e Nakamura (2003) a necessidade de segurança é um fato que vem transcendendo limite da funcionalidade e produtividade. Velocidade e eficiência nos processos de negócio significam vantagem competitiva, enquanto a falta de segurança pode resultar em grandes prejuízos e falta de oportunidades nos negócios.

Segundo a norma ABNT NBR ISO/IEC 27002 (2005) as informações e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação são atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado.

Ainda segundo a norma muitos sistemas não foram feitos para serem seguros. A segurança pode ser alcançada por meios técnicos é limita e requer um planejamento cuidadoso e atenção a detalhes.

Neste sentido foi elaborado um *checklist* com base na norma ABNT NBR ISO/IEC 27002:2005 para aplicação nos Supermercados Myatã LTDA buscando analisar o estado da segurança da informação e ajudar a melhorá-la.

1.2 Objetivos do trabalho

Os objetivos a seguir constituem a finalidade do trabalho científico, ou seja, a meta que se pretende atingir com a elaboração da pesquisa.

1.3.1 Objetivo geral

• Aplicar um *checklist* para verificar o estado da segurança da informação com base na norma ABNT NBR ISO/IEC 27002:2005 nos Supermercados Myatã LTDA.

1.3.2 Objetivos específicos

• Apresentar a norma ABNT NBR ISO/IEC 27002:2005.

• Analisar a segurança da informação e os fatores que a ameaçam.

• Levantar todos os requisitos referentes a segurança da informação de acordo com a norma ABNT NBR ISO/IEC 27002:2005.

1.4 Metodologia

1.4.1 Caracterizações da pesquisa

Para dar início ao trabalho, foi feita uma pesquisa bibliográfica sobre o tema, que acabou por acumular muito material, por esse motivo foi feito uma revisão de todo o conteúdo coletado. Segundo Lakatos (1992) o objetivo da pesquisa é chegar às respostas para as questões propostas mediante o emprego de procedimentos científicos. Toda pesquisa implica em levantamento de dados.

Esta pesquisa pode ser classificada quanto aos objetivos como exploratória, pois, visa proporcionar maior familiaridade com o conteúdo abordado e ainda uma pesquisa experimental, pois busca analisar os resultados da aplicação de um *checklist.* Quanto aos procedimentos a pesquisa é bibliográfica, utilizando-se de livros e artigos revisados relacionados com segurança da informação. A maior fonte de conteúdo é a norma ABNT NBR ISO/IEC 27002:2005. Segundo Gil (1999) a pesquisa bibliográfica é elaborada através de material já publicado com livros e artigos de periódicos estando ou não em meios eletrônicos.

Depois de organizado as informações seguiu a elaboração do *checklist* com base na norma ABNT NBR ISO/IEC 27002:2005. Realizado o experimento nos Supermercados

Myatã LTDA, foi feito uma análise do resultado do teste e apresentado uma possível lista de melhorias na segurança da informação.

1.4.2 Estrutura do trabalho

O trabalho está organizado da seguinte forma:

O primeiro capítulo traz a introdução, apresentando o tema da pesquisa, as questões de estudo, os objetivos, bem como, as justificativas e a sistematização do trabalho.

O segundo capítulo apresenta a revisão da literatura abordando conceitos sobre a informação, ciclo de vida, segurança da informação e suas ameaças mais comuns. O terceiro capítulo traz as práticas que podem ser aplicadas as redes e sistemas de informação. O quarto capítulo traz a norma ABNT NBR ISO/IEC 27002:2005 e seus objetivos. Na sequencia há o *checklist* aplicado aos Supermercados Myatã LTDA e os resultados obtidos. Ao final do trabalho serão apresentadas as referências utilizadas juntamente com os anexos pertinentes.

1.4.3 Cronograma

Atividades Realizadas	Jul	Ago	Set	Out	Nov	Dez
Pesquisa	X					
Apresentação da pré-proposta		X				
Revisão bibliográfica		X				
Elaboração do check-list			X			
Implementação do check-list			X	X		
Relatório dos resultados obtidos				X		
Entrega do TCC à banca examinadora					X	
Correções					X	
Entrega do TCC à banca examinadora						X

Tabela Erro! Indicador não definido. **– Cronograma**
Fonte: Autoria própria.

2 REVISÃO BIBLIOGRÁFICA

2.1 Informação

Segundo a norma ABNT NBR ISO/IEC 27002 (2005) a informação é um ativo que como qualquer outro é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. É especialmente importante no ambiente de negócios, cada vez mais interconectado. Como resultado a informação está cada vez mais exposta a um crescente número e variedades de ameaças e vulnerabilidades.

Para Sêmola (2003) a informação é um conjunto de dados utilizado para a troca de mensagens entre indivíduos ou máquinas em processos comunicativos ou transicionais.

Desde os primórdios foi uma necessidade para o homem comunicar-se e disseminar a informação seja ela de forma escrita, visual ou falada. Hoje "A informação representa a inteligência competitiva dos negócios e é reconhecido como ativo crítico para a continuidade operacional e saúde da empresa" (Sêmola, 2003, p.39). A informação é o principal patrimônio das empresas e está sob constante risco. As informações contêm valor, pois estão integradas com os processos, pessoas e tecnologias.

> Seja para um supermercadista preocupado com a gestão de seu estoque, seja para uma instituição bancária em busca da automação de suas agências, ou para uma indústria alimentícia prospectando a otimização de sua linha de produção, todos decidem suas ações e seus planos com base em informações (SÊMOLA, 2003, p.2).

Ela é o diferencial das empresas para destacar-se no mercado e manter sua competitividade. Dispor da informação correta na hora adequada significa tomar uma decisão ágil e eficiente. (Dias, 2000).

2.1.1 Classificação da informação

Algumas informações são tão importantes que qualquer custo aplicado para a integridade das mesmas é menor do que os de não poder usufruir das informações corretas, entretanto nem todas são vitais. Wadlow (2000) classifica as informações pelo nível de prioridade que respeitam a necessidade de cada empresa bem como a importância que a informação exerce na manutenção das atividades. Seriam:

Pública: Informações que podem vir a serem públicas sem maiores consequências danosas ao funcionamento da empresa.

Interna: Informação que a organização não tem interesse em divulgar, cujo acesso por parte de indivíduos externos deve ser evitado. Sua integridade é importante embora não seja vital.

Confidencial: Informação interna da organização restrita aos limites da empresa cuja divulgação pode causar danos financeiros ou à imagem da empresa. A divulgação pode gerar vantagens a concorrentes e perda de clientes.

Secreta: Informação crítica para as atividades da empresa, restrita a um grupo seleto dentro da organização. Sua integridade deve ser preservada a qualquer custo e acesso bastante limitado e seguro. A segurança deste tipo de informação é vital para companhia.

2.1.2 Ciclo de vida da informação

O ciclo de vida da informação é identificado pelos momentos vividos pela informação que a colocam em riscos. Os momentos são vivenciados justamente quando se faz uso da informação de alguma forma. São quatro os momentos do ciclo da vida onde a informação é exposta a riscos com sua segurança:

• Manipulação ou manuseio: momento em que a informação é criada e manipulada. É a fase onde há maior interação entre as entidades. É onde ocorre a maioria das falhas de segurança, seja a folhear papeis, digitar informações em um aplicativo ou utilizar a senha de acesso para autenticação.

• Armazenamento: Refere-se ao armazenamento e arquivamento da informação em meios digitais, magnéticos ou qualquer outro suporte. Durante esta fase a informação deve estar salva e dispor de cópia de segurança e livre dos riscos a segurança física, pois estão sujeitas a riscos ambientais, naturais ou não.

• Transporte: momento em que a informação é transportada seja entre processos, mídias ou entidades internas ou externas. Quando em transporte estão fora do perímetro de segurança do ambiente que a suporta. Requer atenção especial.

• Descarte: momento em que a informação é descartada seja ao depositar na lixeira da empresa ou eliminar um arquivo eletrônico. Quando se descarta o meio que suporta a informação não esta descartando a mesma.

A informação deve ser protegida durante todo seu ciclo de vida, os requisitos podem variar, portanto, devem ser investidos esforços adequados a proteção que se fazer necessário.

2.1.3 Ativos da informação

É usual a visão de que a informação se constitui de um ativo, embora seja uma relação obvia deve-se levar em consideração a relevância da participação dos conjuntos de indivíduos, compostos tecnológicos e processos envolvidos em algumas etapas do ciclo de vida da informação. (Sêmola, 2003).

É comum dar especial atenção aos ativos específicos, como os mais caros e menos comuns, entretanto, quanto maior a participação do ativo no ciclo de vida maior a importância com o qual o ativo deve ser considerado na segurança da informação. Neste sentido mesmo os ativos considerados de baixo valor ou muito comuns podem gerar impacto decisivo sobre a segurança da informação a qual pertencem. Assim pessoas, sistemas, equipamentos e o fluxo da informação devem ser devidamente considerados no planejamento da segurança da informação.

Uma vez que a informação seja considerada sensível, deve-se realizar uma abstração quanto ao conteúdo, volume e formato a fim de se planejar a melhor forma de protegê-la.

2.2 Evolução da internet

Segundo Tanenbaum (2003) a internet não é uma rede, mas sim um vasto conjunto de redes que utilizam certos protocolos comuns. É um sistema pouco usual no sentido de não ter sido planejado nem controlado por ninguém.

Os computadores começaram a tomar o lugar dos mainframes, chegaram desde o ambiente de escritório até servidores de grande porte, quebrou o paradigma de acesso local a informação e chegaram a qualquer lugar do mundo com os notebooks e através da internet. (Semola, 2003).

O crescimento da internet foi explosivo e atualmente há bem mais de 9 milhões de computadores *hosts* que suportam milhões de usuários. A cada mês a internet incorpora milhões de novos usuários, por esse motivo ela começou a ser visada por ladrões que atacam digitalmente.

2.3 Segurança da informação

Segundo a norma ABNT NBR ISO/IEC 27002 (2005) segurança na informação é a proteção da informação dos vários tipos de ameaças para garantir a continuidade do negócio,

minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades.

Desde que o homem descobriu a comunicação existe a preocupação de proteger as informações trocadas. Segundo Kahn (2004) alguns monumentos criados pelo arquiteto egípcio Khnumhotep foram documentados de forma codificada substituindo palavras e trechos do texto em tabuas de argila, caso a tabua fosse roubada o ladrão nunca conseguiria achar o caminho que levava ao tesouro dentro da pirâmide.

Depois da primeira guerra mundial e no inicio da segunda guerra, diversos países desenvolveram códigos de guerra que nada mais eram do que sistemas de comunicação criptografados a fim de comunicar-se entre as tropas e evitar que suas mensagens fossem interceptadas.

Com o surgimento da informática em meados de 1940 já existia a preocupação com a segurança dos sistemas. Já se pensava em interligar computadores e seus sistemas para transmitir dados através de uma rede, as informações passaram a se propagar com maior velocidade e com isso surgiu a necessidade de fazer com que as informações não se perdessem e nem interceptadas.

Segundo Stallings (2002) antes do uso generalizado de equipamentos de processamento de dados a segurança da informação era feita principalmente por meios físicos e administrativos. Um exemplo é o uso de armários para arquivos com fechadura de segredo para armazenas documentos sigilosos e importantes. Hoje se tornou evidente a necessidade de ferramentas automatizadas para proteger arquivos e outras informações. Com a introdução dos sistemas distribuídos e o uso das redes tornaram-se necessárias medidas de segurança para proteger a informação durante a sua transmissão.

Segundo Geus e Nakamura (2003) investir em segurança e indispensável para a sobrevivência e lucratividade da empresa uma vez que a informação é seu bem mais precioso. Segurança é a tentativa de minimizar perdas em uma situação estável, é um processo e não uma tecnologia que se pode comprar.

Para manter-se e conseguir maior segurança é necessário um esforço contínuo a fim de administrar um nível aceitável de risco, um processo cem por cento seguro não existe (Wadlow, 2000).

Conforme a ABNT NBR ISO/IEC 27002 (2005) há três princípios básicos para garantir a segurança da informação:

- Confidencialidade: propriedade que limita o acesso à informação tão somente as entidades legitimas, ou seja, aqueles autorizados pelo proprietário. É a proteção para

impedir que pessoas não autorizadas tenham acesso e acabem divulgando o conteúdo da informação.

- Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantias do ciclo de vida. É a proteção contra modificações intencionais ou acidentais não autorizadas.
- Disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Adachi (2004) classifica a segurança da informação em três camadas:

- Camada Física: referente aos ambientes onde se encontram o *hardware* podendo ser um escritório, fábrica ou a residência de um usuário em caso de acesso remoto. Segundo Caruso e Steffen (1999) A segurança física relaciona-se diretamente com os aspectos associados ao acesso físico a recursos de informações, tais como disponibilidade física sejam esses recursos as próprias informações seus meios de suporte e armazenamento ou mecanismos de controle de acesso as informações.
- Camada Lógica: caracteriza-se pelo uso de *softwares* responsáveis por funcionalidades do *hardware,* pela realização de transações em base de dados, etc. A segurança em nível lógico refere-se ao acesso que os usuários têm as aplicações dos ambientes informatizados.
- Camada Humana: refere-se a todos os recursos humanos presente nas organizações principalmente os que têm acesso de tecnologia da informação, seja manutenção ou uso. Segundo Scheneier (2001) esta é a camada mais difícil de avaliar os riscos e gerenciar a segurança, pois envolve o fator humano com características psicológicas, sócios culturais e emocionais que variam de forma individual.

2.4 Ameaças

Segundo a ABNT NBR ISO/IEC 27002 (2005) as organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças a segurança da informação incluindo fraudes, eletrônicas, espionagem, sabotagem, vandalismo, incêndio.

Danos causados por códigos maliciosos, hackers e ataques de denial of service estão se tornando cada vez mais comuns e incrivelmente sofisticados.

Com o advento das redes de longo alcance surgiu uma característica complicadora a segurança da informação: a capacidade do anonimato. Por esse motivo, em muitos casos, fica obrigado a adoção de mecanismos de identidade eletrônica, certificação digital e outros meios para a identificação segura de usuários.

Para Sêmola (2003) as ameaças podem ser definidas como agentes ou condições que comprometam as informações por meio das vulnerabilidades, provocando a perca de confidencialidade, integridade e disponibilidade.

Existem os seguintes tipos de ameaças.

- Destruição, modificação ou acesso indevido de informação ou outros recursos.
- Interrupção de serviços.
- Roubo ou perda da informação.
- Revelação da informação.

Ainda como ameaças da segurança física e lógica, uma vez que atinja locais de armazenamento, manuseio e transmissão, de informações:

- Água (vazamentos, corrosão, enchentes).
- Eventos catastróficos naturais
- Sabotagem e vandalismo.
- Explosões.
- Roubos.
- Materiais tóxicos.
- Interrupções de energia e comunicação.
- Falhas em equipamentos.

2.5 Ataque

Segundo Stallings (2002) um ataque à segurança do sistema é derivado de uma ameaça inteligente, ou seja, um ato inteligente é uma tentativa deliberada de burlar os serviços de segurança e violar a política de um sistema.

Conforme Honório (2003) os ataques podem ser intencionais ou acidentais, podendo ser ativos ou passivos.

• Acidentais: são ataques sem intenção não planejados anteriormente.

• Intencionais: são ataques com intenção de causar danos, planejados anteriormente.

• Passivos: possuem a natureza de bisbilhotar arquivos ou transmissões. O objetivo é obter informações que estão sendo guardadas ou transmitidas.

• Ativos: envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso.

Um ataque corresponde à concretização de uma ameaça não necessariamente bem sucedida. A geração de ataques é originada por pessoas ainda que utilize os recursos computacionais e sua prevenção tornou-se extremamente complexa. Segundo Shell (2001) não existe ciência que seja capaz de eliminar os incidentes de segurança restante a opção da constante vigilância e verificação.

Os ataques podem ser de origem externa ou interna. Para Schultz (2002) os ataques de origem interna são em maior numero que os externos, possuem motivações e padrões diversos, exigindo analise e contra medidas diferentes.

Segundo Stallings (2002) os possíveis ataques em sistema podem ser classificados como:

• Ataque de interrupção: visa destruir ou interromper o serviço oferecido, ou seja, a disponibilidade das informações. É um desvio ou interrupção do fluxo normal das mensagens ao destino.

• Ataque de interceptação: tem como objetivo capturar o que esta sendo transmitido sem que o sistema perceba. A entidade não autorizada pode ser uma pessoa, um programa ou computador.

• Ataque de modificação: acontece quando existe alteração da informação que esta sendo transmitida por entidades não autorizadas violando a integridade das informações.

• Ataque de falsificação: o atacante tem como finalidade se passar por usuário do sistema a fim de obter informações e transmitir falsos dados na rede. Ataca a autenticidade da informação.

2.5.1 Principais ataques

Vírus: tem relação com os vírus da biologia, não podem agir sozinhos, tem a propriedade de anexar-se a outros arquivos, alterar seu funcionamento normal e se reproduzir. São códigos maliciosos que forçam a duplicação automática para aumentar o poder de ataque. Podem infectar todos os tipos de arquivos. (Barbosa, 2004).

Worms: Segundo Laureano (2005) funciona de maneira similar aos vírus, entretanto não precisam de outros arquivos para se duplicar e invadirem aproveitam as falhas de segurança do sistema e disseminam-se por meio de redes de segurança.

Trojan: Tipo de *malware* baixado pelo usuário sem que ele saiba, geralmente são programas disfarçados que ao serem executados efetuam tarefas maliciosas e alteram o sistema para permitir ataques posteriores. O *trojan* não se replica ele só é propagado por intervenção humana (Andrade, 2005).

Spyware: São aplicativos instalados sem o consentimento do usuário utilizados para capturar informações de utilização e navegação enviando *logs* aos invasores.

Keyloggers: Aplicativos usados para roubo de informações bancárias. Aplicativos ocultos instalados no computador e geram relatórios completo de tudo que é digitado na máquina.

Exploit: Programa criado para explorar uma falha de segurança do sistema. Pode servir para obter acesso indevido ou tirar um sistema do ar (Andrade, 2005).

Rootkit: Segundo Barbosa (2004) é um para *malware* que se esconde na base do sistema operacional projetado para não deixar pistas de um invasor em localidades que os antivírus não podem encontrá-los. Utilizados para interceptar solicitações do sistema e alterar resultados.

Adware: Arquivo malicioso que nem sempre são baixados por acidente, alguns são carregados em propagandas que só as eliminam após a aquisição de uma licença. Baixa ou exibe, sem autorização, anúncios na tela do computador.

Scareware: *malware* escondidos em baners maliciosos com informações do tipo “você esta infectado, clique aqui para limpar sua maquina”.

Phising: *email* enviado por *spammers* criados com interfaces e nomes que fazem referencia a empresas famosas. Onde são colocados *links* disfarçados que na verdade são arquivos maliciosos.

Estouro de *buffer*: faz com que um programa modifique o final de uma área de armazenamento de dados, assim o invasor pode sobre-escrever parte do programa e executar

seu código. Problema principalmente encontrado em programas das linguagens c e c++. (Andrade, 2005).

Hacker: Usuários que buscam brechas e falhas de segurança em sistemas, utilizando esses meios desenvolvem suas capacidades e conhecimento em programação.

Cracker: Usuário que assim como o *hacker* busca brechas e falhas de segurança, entretanto, utilizam estes conhecimentos para causar danos.

Sniffers: Segundo Honório (2003) são programas que verificam o trafego na rede, são uteis para o gerenciamento de redes, capturam os pacotes trocados na rede. Se os dados não forem criptografados podem ser usados para roubos de senha e informações sigilosas, conversas e outros *logs* registrados no computador, é muito difícil de ser detectado, pois se trata de uma invasão passiva. Os *sniffers* não podem ser considerados ataques porque são usados para diagnosticar problemas de rede.

Drive-to-java: Aplicativos maliciosos "*drive-to-download*" que invadem os computadores quando usuários clicam sobre anúncios que direcionam a *downloads* sem autorização, ocorre principalmente em aplicativos Java.

DNS poisoning: "Envenenamento do DNS" os usuários atingidos conseguem navegar normalmente pela internet, mas os dados são enviados para um computador invasor intermediário.

Data Modification: alteração de dados. Decodificar pacotes capturados e modificar as informações contidas antes de chegar ao destinatário.

Spoofing: é o ato de mascarar informações para evitar rastreamento, forjando o endereço de origem de um ou mais *hosts* empenhados na autenticação das maquinas individualmente.

Denial of service: Ataque de negação em serviços. Consiste em sobrecarregar um servidor com uma quantidade excessiva de serviços. Alvos mais frequentes são servidores *web*. As consequências mais comuns são consumo excessivo de recursos e falhas na comunicação. (Andrade, 2005).

Spam: mensagens criadas para uma lista de maneira ilegal, geralmente sobre propagandas e pirataria.

Man-in-the-midlle-attack: quando um computador intercepta a conexão de outros dois. O invasor se esconde com a máscara de ambos e pode interceptar uma conversa e comunicar-se com os dois usuários ao mesmo tempo.

Engenharia social: Segundo Nakamura e Geus (2003) é o ato de manipular pessoas para conseguir informações confidenciais sobre brechas de segurança tem como objetivo

enganar e ludibriar pessoas assumindo uma falsa identidade.

Bloatware: programas que causam perda do espaço livre nos computadores por serem maiores do que deveriam ser não são aplicativos de invasão.

IMCP attack: ataques gerados nos protocolos de controle de mensagens de erro de internet. Consiste em enviar centenas ou milhares de erros para servidores remotos que irão enviar respostas para o endereço com a mesma intensidade causando travamento na conexão e quedas.

Password-based-attacks: ataque gerado por programas no intuito de tentar senhas repetidas vezes em certos intervalos de tempo.

Repudiation attacks: sistemas não criados com os comandos corretos de rastreamento de *logs* podem ser modificados os dados de endereçamento das informações.

Compromised-key attack: realizados para determinadas chaves do registro do SO. Quando consegue acesso às chaves podem ser modificadas para gerar *logs* com a decodificação das senhas e invadir contas e serviços.

Ping of death: Segundo Laureano (2005) o invasor realiza constantes pings com tamanho maior que o máximo permitido ocasionando travamentos na banda e do computador, outras abortam e mostram mensagens de erro. Praticamente todas as plataformas são afetadas por esse ataque.

Scanners de portas: *softwares* que varrem computadores em buscar de portas TCP abertas para uma possível invasão. Para que não sejam detectados alguns programas testam as portas em horários aleatórios.

Session hijacking: roubo de sessão. Usuário malicioso intercepta *cookies* com dados de algum serviço online e com isso consegue acessar a pagina do serviço como se fosse a vitima.

Phreaker: *hackers* de telefonia roubam sinal de outros aparelhos e também desbloquear aparelhos com proteções.

Honeypot: armadilha para *hackers*. Configura-se um servidor de isca, deixando brechas para invasão, os *softwares* coletam informações sobre o invasor.

2.6 Vulnerabilidades

Segundo Wadlow (2000) vulnerabilidades são os elementos que ao serem explorados afetam os princípios básicos da informação: a confidencialidade, a disponibilidade e a integridade. Em segurança da informação um dos primeiros passos é rastrear e eliminar os

pontos fracos de um ambiente da tecnologia da informação.

As vulnerabilidades são fragilidades presentes ligadas a ativos que controlam e processam informações, que se exploradas podem ocasionar incidentes de segurança, tendo sempre um agente causador que favoreça o incidente. (Sêmola, 2003).

As diferentes soluções tecnológicas utilizadas na redução de vulnerabilidades estão geralmente orientadas a problemas específicos e sua utilização pode introduzir novas vulnerabilidades. Diversas soluções surgiram ao longo do tempo, entretanto são diretamente dependentes dos recursos tecnológicos e podem de certa forma estar sujeitas a vulnerabilidades, realimentando o ciclo da procura por soluções efetivas ao problema.

2.7 Riscos

O risco deve ser adequadamente medido e avaliado possibilitando a criação de medidas preventivas para a sua diminuição. Segundo Dawel (2003) os riscos podem ser definidos como as perdas de qualquer modo que podem ocorrer como consequência de um determinado curso de ação. Pode-se medir o risco com a unidade monetária envolvida ou pela probabilidade de perdas e ganhos associados a alguma alternativa em particular. O risco jamais poderá ser eliminado.

A norma ABNT NBR ISO/IEC 27002 (2005) diz que os requisitos da segurança da informação são identificados por meio de uma analise sistemática dos riscos da segurança da informação. Os resultados ajudarão a direcionar e determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos de segurança e para a proteção contra riscos. Convém que a analise de riscos seja repetida periódicamente para contemplar quaisquer mudanças que possam influenciar os resultados.

Segundo Dawel (2003) a gestão de riscos deve identificar as eventuais fraquezas e seus valores, permitir que a gerência tome decisões fundamentais sobre a gestão e incrementar a informação organizacional sobre os sistemas a fim de melhorar a segurança.

A avaliação de riscos compreende nove passos (Dawel, 2003):

- Caracterização do sistema.
- Identificação de ameaças.
- Identificação de vulnerabilidades.
- Analise de controles utilizados.
- Determinação da probabilidade dos possíveis eventos contra a segurança.

- Analise de impacto.
- Determinação dos riscos.
- Recomendações de controles a utilizar.
- Documentação dos resultados.

3 PROTEÇÃO

A segurança da informação dispõe de diversos métodos e ferramentas para diminuir os riscos e possíveis ataques à informação, visando proteger os princípios básicos – confidencialidade, integridade e disponibilidade.

3.1 Ambiente físico

Segundo Silva, Carvalho e Torres (2003) o ambiente físico pode constituir um dos elementos mais importantes no que diz respeito a salvaguarda da informação.

3.1.1 Áreas

Para Silva, Carvalho e Torres (2003) em zonas densamente povoadas como os grandes centros urbanos a escolha da localização da empresa é muito importante, pois contribui decisivamente na construção de ambientes seguros. Os componentes críticos de armazenamento, processamento ou transmissão não deverão encontrar-se ser de acesso demasiado fácil. A segurança física deverá ser pensada em moldes concêntricos de profundidade, com o objetivo de incrementar os níveis de proteção contra acessos não autorizados. Os níveis de validação devem ser igualmente proporcionais à informação que protegem.

3.1.2 Localização dos centros de dados

A localização dos centros de dados devera ser considerada. Existem várias linhas de orientação que deverão ser seguidas para a localização e configuração de um CPD.

Segundo Silva, Carvalho e Torres (2003) estas são algumas características que devem ser observadas:

- O CPD não deverá ficar nem no térreo nem no ultimo piso do edifício, no caso de edifícios térreos deverá se localizar no centro longe das vias de circulação publica e não devem existir acessos ao exterior e os acessos existentes deverão ser monitorados.
- Não deverão existir condutos de água ou de esgoto nas imediações dos centros de dados.
- Deverão existir sistemas de alimentação elétrica redundantes além de condutos necessários à alimentação elétrica e processamento da atmosfera.
- Os sistemas de detecção e combate a incêndios deverão ser apropriados.

Estas orientações permitem a criação de centros de TI conforme as mais exigentes normas de segurança, mas nem todas as situações permitem o cumprimento das orientações. No caso de instalações já existentes surge a necessidade de fazer o melhor possível com o que já existe.

3.1.3 Controle de acessos

O controle de quem entra e quem sai das instalações é um aspecto importante da segurança física. Não basta policiar somente a entrada de pessoas, mas também garantir que os visitantes não levem material da empresa sem autorização.

O controle de acesso não se resume a portaria com guardas e um sistema de vídeo em circuito fechado. O controle deve abranger todas as áreas sensíveis, os arquivos centrais e os centros de dados e deverá ser abrangente na medida em que não houver exceções. Nenhuma medida porem fará sentido sem o devido acompanhamento.

3.1.4 Eliminação de resíduos

Segundo Silva, Carvalho e Torres (2003) os resíduos que deixaram de possuir interesse são eliminados, porem, nem sempre é a ação mais indicada e pode criar potenciais compromissos à segurança da empresa. Uma disciplina muito popular entre *hackers* a ”*dumpote diving*” consiste em vasculhar os depósitos de lixo eletrônico em busca de informações valiosas que poderão constituir uma forma de ataque futuro, seja físico ou digital.

3.1.5 Rastros

Segundo Silva, Carvalho e Torres (2003) o rastro é o registro de qualquer atividade monitorada nas instalações de uma organização. Podem ser compostos pelos mais diversos elementos. É o rastro que permite reconstituir qualquer evento ocorrido e todos os registros devem ser guardados por um determinado período de tempo dado a sua importância. Somente com os registros é possível identificar, investigar e eventualmente evitar potenciais falhas de segurança.

3.2 Segurança lógica/física

Segundo Gil (1998) sem a existência de medidas de segurança lógica a informação fica exposta a ataques, alguns são passivos na medida em que apenas capturam os dados, enquanto outros ativos afetando a informação. O catalogo de ataques é demasiado volumoso e a tendência é piorar. Esta e a área mais complexa da segurança empresarial a medida que se sucedem as gerações tecnológicas, assim como sua complexidade. Existem três áreas que se destacam neste campo: a prevenção, a proteção e a reação.

3.2.1 Autenticação e controle de acessos

Segundo Ferreira e Araújo (2006) o processo mais adequado para se manter o controle sobre os acessos aos sistemas é propor processos com intervalos periódicos para a revisão das contas de usuário.

A autenticação e o controle de acesso são aspectos importantes na vida cotidiana, um cheque é autenticado com a assinatura do titular, em um caixa eletrônico utiliza-se uma senha e um cartão para acessar a conta. Nos SI a autenticação e o controle são igualmente importantes, são eles que asseguram quem somos e que tipo de acesso temos, ao nível de redes de comunicações ou ao nível de aplicação. (Silva, Carvalho e Torre, 2003).

Cada usuário deve possuir uma única identificação, todos os usuários necessitam de uma identificação. Por meio destes métodos permite-se um controle das ações praticadas por cada usuário. (Dias, 2000).

A grande questão que se coloca é a melhor forma de autenticar alguém e garantir que apenas as pessoas autorizadas tenham acesso. Segundo Dias (2000) logo após a identificação do *login* o sistema identifica se é ele mesmo ou não. Essa autenticação do usuário acontece através de seu ID e uma senha pessoal e intransferível.

3.2.1.1 Senhas

Para Silva, Carvalho e Torres (2003) as senhas são atualmente a norma mais comumente utilizada pata a autenticação de qualquer usuário em um sistema. Esta solução levanta vários problemas. A gestão de senhas pode facilmente tornar-se um quebra-cabeça, devido à quantidade de senhas que uma pessoa precisa estar à memória. É natural que o usuário opte por soluções mais fáceis como a utilização de uma senha igual a todos os serviços ou simplesmente a manutenção de uma lista escrita, tornando-se uma vulnerabilidade.

Segundo Ferreira e Araújo (2006) uma boa senha deve conter pelo menos seis caracteres, simples de digitar e fácil de lembrar. Senhas que misturam caracteres, que não utilizem palavras do dicionário e nem nomes de familiares reforçam o bloqueio de acesso das informações.

3.2.1.2 Smart Card

As senhas são um mal necessário, por esse motivo buscam-se maneiras de substituir por formas mais simples e seguras.

Segundo Silva, Carvalho e Torres (2003) outra opção e o uso de *smart cards* (cartões inteligentes) que não associa mais a algo que o usuário sabe, mas sim a algo que ele possui. O *smart card* é um cartão com circuito integrado capaz de armazenar dados de forma segura, tais como, certificados digitais ou chaves criptográficas protegidas por um PIN. Com essa capacidade, alem da diversificação dos códigos de autenticação e o isolamento dos elementos de segurança os *smart cards* acrescentam um nível de segurança em relação com as senhas digitadas.

3.2.1.3 Biometria

A biometria é a utilização de características biológicas em mecanismos de identificação. Na biometria os identificadores são obtidos através de singularidades pertencentes a características biológicas. Essas características podem ser físicas (olhos, digitais) ou comportamentais (modo como assina um documento).

Segundo Silva, Carvalho e Torres (2003) há de ponderar os elementos associados a esta tecnologia, a falta de aceitação por parte dos utilizadores em que a empresa fique com

registros de suas características físicas.

3.2.2 Criptografia

Segundo Forouzan (2006) a palavra criptografia refere-se à ciência e a arte da transformação de mensagens tornando-as seguras e imunes a ataques. A mensagem original antes de ser codificada é denominada texto limpo, após a transformação é conhecido como texto cifrado sendo necessário um algoritmo de decifragem para revelar a mensagem original.

Segundo Silva, Carvalho e Torres (2003) a cifra é o processo pelo qual se protege um conjunto de dados de modo que só alguém que conheça o segredo possa conhecer o conteúdo da mensagem ou dados. O algoritmo e tão mais poderoso quanto melhor a chave e mais resistente a tentativas de quebra do segredo.

Para Forouzan (2006) todos os algoritmos de criptografia foram separados em dois grupos: algoritmos de chave simétrica ou privada e algoritmos de chave assimétrica ou publica. No caso das chaves o nível de segurança de uma criptografia é medido no número de bits, ou seja, quanto mais bits forem usados, mais difícil será quebrar a criptografia na força bruta. Se tivermos uma criptografia de 10 bits, existirão apenas 2^{10} (ou 1024) chaves, porém, ao usarmos 64 bits, o número de chaves possíveis subirá para aproximadamente 20 x 10^18 chaves, um número alto até mesmo para um computador.

No caso da função *Hash*, o nível de segurança é dado pela dificuldade de se criar colisões intencionais, evitando que haja sequência iguais para dados diferentes. A chave, na criptografia de chave pública, é baseada em um *hash value*. Esse é um valor que é calculado a partir de um número de entrada baixo utilizando um algoritmo de espalhamento. O importante é que se torne quase impossível derivar o número original de entrada sem conhecer os dados utilizados para criá-lo.

As chaves públicas geralmente utilizam algoritmos complexos e *hash value* muito grandes para criptografia, incluindo números de 40 bits ou até mesmo de 128 bits. Um número de 128 bits possui cerca de 2^{128} combinações ou $340x10^{27}$ diferentes combinações possíveis.

3.2.2.1 Chave simétrica

Segundo Guedes (2000) se tanto o emissor quanto o receptor em uma comunicação

criptografada utilizam a mesma chave o sistema é simétrico, de única chave ou sistema de criptografia convencional. A criptografia simétrica baseia-se na simetria das chaves, ou seja, a mesma chave utilizada para criptografar será usada para decodificar a mensagem.

Segundo Sêmola (2003) este tipo de criptografia tem uma vulnerabilidade, pois, ao criar a chave e envia-la junto a mensagem ao destinatário ela não está protegida comprometendo a confidencialidade.

3.2.2.2 Chave assimétrica

Segundo Guedes (2000) a criptografia assimétrica envolve o uso de duas chaves distintas, uma privada e outra pública. Pode-se utilizar qualquer uma das chaves para cifrar a mensagem, entretanto somente a chave inversa deve ser utilizada para decifra-la.

As desvantagens se devem ao fato de que apenas uma chave é utilizada para cada par de entidades a segurança deve ser mais rigorosa e quanto maior o numero de entidades comunicando-se mais difícil a gerencia das chaves, pois, cada comunicação irá necessitar uma cópia das chaves (Dias, 2000).

3.2.3 IPv6

O IPv6 encontra-se em fase de desenvolvimento, surgiu com a necessidade de criação de um novo esquema de atribuição de endereços uma vez que o esquema atual o IPv4 encontra-se quase esgotado. No seu desenvolvimento os grupos envolvidos aproveitaram para aperfeiçoar o protocolo introduzindo capacidades de regulação da qualidade de serviços de autenticação e privacidade. Inclui definições de extensões que suportam as necessidades de autenticação, integridade e confidencialidade das comunicações ao nível de protocolo. (Silva, Carvalho e Torres, 2003).

3.2.4 *Firewall*

Segundo Cheswick, Bellovin e Rubin (2005) o *firewall* é uma coleção de componentes colocados entre duas redes que possui as seguintes propriedades:

- Todo o trafego de dentro para fora e vice-versa, deve passar pelo *firewall*.
- Apenas trafego autorizado, como definido pela política de segurança local, terá

permissão de passar.

• O próprio *firewall* deve ser imune a acessos não autorizados.

Para Tanenbaum (2003) os *firewalls* são uma adaptação de antigas formas de segurança medieval: cavar um túnel profundo em torno do castelo, o que forçava todos que queriam entrar ou sair a passar por uma ponte levadiça onde poderiam ser revistados.

Ainda no pensamento de Cheswick, Bellovin e Rubin (2005) a maior razão pelo qual o *firewall* seja mais seguro é simplesmente que ele não é um *host* de uso geral. Um segundo beneficio vem da administração das maquinas de *firewall*, são totalmente configuráveis as necessidades da rede, normalmente não possuem nenhum usuário normal apenas o administrador.

3.2.5 Antivírus

Segundo Silva, Carvalho e Torres (2003) poucas empresas não utilizam de forma coordenada, qualquer mecanismo antivírus em seus sistemas. Os antivírus existentes baseiam-se em assinaturas para cumprir a sua função. Uma assinatura é um pedaço do código binário que permite a identificação com uma simples comparação com um banco de dados.

Seguindo o pensamento estas soluções obrigam a permanente atualização das bases de dados de assinaturas e com menos frequência os motores de detecção e remoção. O fato é que sem o devido planejamento prévio o esforço para a atualização pode se tornar uma brecha à medida que aparecem novos vírus mais difíceis de serem removidos e isolados.

3.2.6 Redundância

A redundância é a forma mais obvia de evitar a indisponibilidade da informação. Existem mecanismos de complexidade variável que permitem criar copias da informação contida nos sistemas. A redundância pode ser obtida através de copias manuais ou sistemas automatizados de proteção da informação. Esses mecanismos duplicam toda a infraestrutura do sistema, em uma localização remota, com transferência automática de dados entre os locais. (Silva, Carvalho e Torres, 2003).

3.2.7 *Backup*

O *backup* é uma copia de segurança dos arquivos importantes da empresa. Segundo

Júnior (2007) as copias de segurança em computadores são instrumentos importantes para compensar falhas em *hardware* ou *software*, como uma invasão do sistema, ataques de vírus, perda acidental de arquivos, etc. A cópia de segurança e a melhor forma de prevenção e recuperação das informações, já que os dados podem voltar facilmente para o disco. Para Ferreira e Araújo (2006) cabe a instituição levar em consideração a importância da informação que tem levando em conta sua periodicidade e volatilidade.

A frequência do *backup* depende diretamente da relevância que os dados possuem, assim como a quantidade de informações que serão processadas. (Júnior, 2007).

4 NORMA ABNT ISO/IEC 27002:2005

Segundo a Norma ABNT NBR ISO/IEC 27002:2005 a Norma ABNT NBR ISO/IEC 17999:2005 foi elaborada no Comitê Brasileiro de Computadores e Processamento de dados (ABNT/CB-21), pela comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:204.01). O projeto circulou em consulta nacional conforme Edital nº 03 de 31-03-2005 com o número de projeto NBR ISO/IEC 17999. Esta norma equivale a ISO/IEC 27002:2005.

Uma família de normas de sistemas de gestão da segurança da informação está sendo desenvolvida. A família inclui normas sobre requisitos de sistema de gestão da segurança da informação, gestão de riscos, métricas, medidas e diretrizes pela implementação. Esta família adota o sistema de numeração 27000 em sequência.

4.1 Objetivo

A Norma ABNT NBR ISO/IEC 27002 estabeleceu diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos desta norma provêm diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação.

Os objetivos de controle tem como finalidade ser implementados para atender aos requisitos identificados por meio da análise, avaliação dos riscos. Esta norma deve servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança e para ajudar a criar confiança nas atividades organizacionais.

4.2 Capítulos

A norma define 128 controles que compõem o escopo do sistema de gestão da segurança da informação agrupado em 11 seções de controles: organização da segurança da informação, política de segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção dos sistemas de informação; gestão de incidentes da segurança da informação; gestão da continuidade do negócio e conformidade.

4.2.1 Análise/avaliação e tratamento de riscos

Este capítulo está focado nas diretrizes para análise/avaliação e tratamento de riscos. Segundo a norma ABNT NBR ISO/IEC 27002 (2005) convém que a análise, avaliações de riscos, identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos objetivos relevantes para a organização. Com base nos resultados desta análise de riscos a organização pode direcionar a gestão de segurança da informação e os controles apropriados.

Ainda seguindo a norma convêm que a análise/avaliação de riscos inclua enfoque sistemático de estimar a magnitude do risco e o processo de comparar os riscos estimados contra os critérios de risco para determinar a sua significância. Convém ainda que sejam realizados periodicamente e inclua os relacionamentos com as análises de todos os setores da organização.

O capítulo demonstra também as possíveis opções para o tratamento de riscos:

- Aplicar controles apropriados.
- Conhecer e objetivamente aceitar os riscos.
- Evitar riscos, não permitindo ações que possam causá-los.
- Transferir os riscos associados para outras partes.

4.2.2 Política de segurança da informação

Segundo a Norma ABNT NBR ISO/IEC 27002 (2005) o objetivo de uma política de segurança da informação é prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes. Convém que a direção estabeleça uma clara orientação da política, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

É importante que um documento da política de segurança seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. Este documento deve conter uma definição sobre a segurança da informação suas metas, escopo e importância uma declaração do comprometimento da direção apoiando as metas e princípios, breve explanação das políticas, princípios e normas, definição das responsabilidades gerais e específicas na gestão da informação.

De acordo com a Norma ABNT NBR ISO/IEC 27002 (2005) convém que a política de segurança da informação seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem para assegurar a sua continua pertinência adequação e eficácia.

4.2.3 Organizando a segurança da informação

Este capítulo traz diretrizes que tem como objetivo gerenciar a segurança da informação dentro da organização.

Segundo a Norma ABNT NBR ISO/IEC 27002 (2005) convém que a direção da organização aprove a política de segurança da informação, atribua as funções, coordene e analise criticamente a implementação de segurança da informação por toda a organização.

Uma estrutura de gerenciamento deve ser estabelecida para iniciar e controlar a implementação de segurança da informação dentro da organização. Se necessário, pode ser elaborado uma consultoria especializada em segurança da informação seja estabelecido e disponibilizado na organização. Contatos com especialistas ou grupos de segurança da informação externos, incluindo autoridades relevantes sejam feitas para manter-se atualizado com as tendências do mercado, monitorar normas e métodos de avaliação, além de fornecer apoio adequado, quando estiver tratando de incidentes de segurança da informação. Convém um enfoque multidisciplinar na segurança da informação seja incentivado.

4.2.4 Gestão de ativos

De acordo com a Norma ABNT NBR ISO/IEC 27002 (2005) o objetivo da gestão de ativos é alcançar e manter a proteção adequada aos ativos da informação.

Convém que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido, é importante que todas as informações e ativos associados com os recursos de processamento da informação tenham um proprietário, ou seja, um responsável dentro da organização, designado por uma parte definitiva da organização. Todas as regras envolvidas no uso da informação e dos ativos devem ser identificadas e documentadas e implementadas.

O capitulo contém ainda diretrizes sobre a classificação da informação visando assegurar que receba um nível adequado de proteção. Convêm que a informação seja classificada e rotulada em termos do seu valor, requisitos legais, sensibilidade e criticidade

para a organização.

4.2.5 Segurança em recursos humanos

Este capítulo incorpora as diretrizes para assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papeis e reduzir o risco de furto ou roubo, fraude ou mal uso de recursos. Segundo a Norma ABNT NBR ISO/IEC 27002 (2005) existem três pontos importantes na segurança em recursos humanos: Antes da contratação, durante a contratação e encerramento. Seguindo as diretrizes as responsabilidades pela segurança da informação devem estar atribuídas antes da contratação, de forma adequada, nas descrições de cargos e funções, todos os candidatos aos cargos, fornecedores e terceiros devem ser analisados especialmente em cargos ligados a informação sensível. É importante que todos os usuários dos recursos de processamento da informação assinem contratos sobre papeis e responsabilidades (ABNT NBR ISO/IEC 27002:2005).

Durante a contratação é importante um nível adequado de conscientização, educação e treinamento nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação seja para todos os funcionários, fornecedores e terceiros, para minimizar possíveis riscos da informação.

No encerramento de um contrato a organização deve assegurar que a saída seja organizada e que a devolução dos equipamentos e a retirada de todos os direitos do acervo, o mesmo procedimento deve ser efetuado quando há uma mudança de cargo.

4.2.6 Segurança física e do ambiente

Segundo a Norma ANBT NBR ISO/IEC 27002 (2005) o objetivo de áreas seguras é prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização. Convém que as instalações de processamento da informação críticas ou sensíveis sejam mantidas em áreas seguras protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados. Convém que sejam fisicamente protegidas contra o acesso não autorizado, danos e interferências a proteção oferecido deve ser compatível com os riscos identificados.

Quanto a segurança dos equipamentos, é necessário para reduzir o risco de acesso não autorizado as informações e proteger contra perdas ou danos. Deve ser levada em consideração a introdução de equipamentos no local, bem como a remoção. Podem ser

necessários controles especiais para a proteção contra as operações físicas e para proteção de instalações de suporte, com a infraestrutura de suprimento de energia e de cabeamento. Os equipamentos devem ser protegidos contra ameaças físicas e do meio ambiente. Essas diretrizes irão impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das atividades da organização.

4.2.7 Gerenciamento das operações e comunicações

O capitulo contém diretrizes para garantir a operação segura e correta dos recursos de processamento da informação. Segundo a Norma ABNT NBR ISO/IEC 27002 (2005) os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações sejam definidos. Abrange desenvolvimento de procedimentos operacionais apropriados convém que seja utilizada a segregação de funções quando apropriado, para reduzir riscos do mau uso ou uso doloso dos sistemas.

O gerenciamento de serviços terminados relacionados à comunicação tem como objetivo implementar e manter o nível apropriado de segurança da informação de entrega de serviços juntamente com acordos de entrega de serviços terceirizados. A organização deve unificar a implementação dos acordos, montar a conformidade dos acordos e gerenciar as mudanças para garantir que os serviços entregues atendem a todos os requisitos acordados com os terceiros (ABNT NBR ISO/IEC 27002:2005).

De acordo com a norma o planejamento e a preparação prévia são requeridos para garantir a disponibilidade adequada de capacidade e recursos para entrega do desempenho do sistema, as projeções de risco sejam feitos para reduzir o risco de sobrecarga dos sistemas. Todas essas diretrizes visam minimizar o risco de falhas de sistemas.

Dentro da proteção contra códigos maliciosos e códigos móveis as diretrizes visam proteger a integridade do software e da informação. É importante existir precauções para prevenir e detectar a introdução de códigos maliciosos e código não autorizados. Os usuários devem estar conscientes dos perigos do código malicioso. Se apropriado os gestores devem implantar controles para prevenir, detectar e remover códigos maliciosos.

O capitulo também enfoca na importância das cópias de segurança para manter a integridade e disponibilidade da informação. Quanto ao manuseio de mídias convém que sejam controladas e fisicamente protegidas com o objetivo de prevenir contra divulgação autorizada da modificação, remoção ou destruição aos ativos e interrupções das atividades de negócio.

4.2.8 Controle de acessos

De acordo com a norma ABNT NBR ISO/IEC 27002(2005) é importante controlar o acesso a informação, com base nos requisitos de negócio e segurança da informação. As regras de controle de acesso devem levar em consideração as políticas para autorização e disseminação da informação. Devem assegurar acesso de usuários autorizados e prevenir acesso não autorizado com procedimentos formais de controle e distribuição, que entram todas as fases do ciclo de vida de acesso do usuário, da inscrição inicial ate o cancelamento de usuários. A colaboração dos usuários é essencial para uma efetiva segurança, os usuários devem estar conscientes de suas responsabilidades, particularmente em relação ao uso de senhas e de segurança dos equipamentos. Convém que o acesso aos serviços de redes internos e externos seja controlado, assim como o acesso ao sistema operacional. O controle de acesso às aplicações e informação deve ser restrito a usuários autorizados e seja função dos sistemas de aplicação controlar o acesso, proporcionar proteções contra acesso não autorizado e não comprometam outros sistemas com os quais a informação é compartilhada. Em computação móvel e trabalho remoto convém que a proteção requerida seja proporcional com o risco da forma especifica de trabalho.

4.2.9 Aquisição desenvolvimento e manutenção de sistemas de informação

Sistemas de informação incluem sistemas operacionais, infraestrutura, aplicações de negócios, serviços e aplicações desenvolvidas pelo usuário e tem papel importante nos processos de negócio, por esse motivo convém que os requisitos de segurança sejam identificados e abordados antes do desenvolvimento ou implementação de sistemas de informação. É importante que controles apropriados sejam incorporados no projeto das aplicações para assegurar o processamento correto, controles adicionais podem ser necessários para sistemas que processem informações sensíveis, valiosas ou críticas. Ainda podem ser implementados controles criptográficos para proteger a confidencialidade, a autenticidade ou a integridade das informações.

O acesso aos arquivos do sistema deve ser controlado e atividades de projetos de TI e de suporte sejam conduzidas de forma segura. Para manter-se a segurança em processos de desenvolvimento e suporte os ambientes de projeto e suporte devem ser estritamente controlados. Deve existir também uma gestão de vulnerabilidades técnicas e que o mesmo seja implementado de forma objetiva.

4.2.10 Gestão de incidentes de segurança da informação

É importante que as fragilidades e exceções de segurança da informação associados com sistemas de informação sejam comunicados permitindo a tomada de ação corretiva em tempo hábil e assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.

4.2.11 Gestão da continuidade do negócio

Segundo a Norma ABNT NBR ISO/IEC 27002 (2005) o objetivo deste capítulo é demonstrar as diretrizes para que a organização não permita a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil.

4.2.12 Conformidade

É importante evitar violações de quaisquer obrigações legais, estatuários, regulamentares ou contratuais e de quaisquer requisitos de segurança da informação e garantir conformidade dos sistemas com as políticas e normas organizacionais da segurança da informação. Maximizar a eficácia é minimizar a interferência no processo de auditoria dos sistemas de informação.

5 CHECKLIST

5.1 Caracterizações do *checklist*

O *checklist* é de autoria própria e tem suas questões formuladas com base nas diretrizes expostas pela norma ABNT NBR ISO/IEC 27002:2005, abrange todas as seções e subseções da norma, é composto por 161 questões com as alternativas de atinge, atinge parcialmente e não atinge.

O questionário foi aplicado à empresa com a ajuda do gestor de TI que também é o responsável pela política de segurança dos Supermercados Myatã.

5.2 Caracterizações da empresa

Nome: Supermercados Myatã LTDA
Endereço: Av. Papa João XVIII, 353 - Ipiranga.
Cidade: Lages UF: SC
Telefone: (49) 3221-2400
E-mail: myata@supermyata.com.br
Ramo de Atividade: Alimentício
Objetivo Empresarial: Lucro
Porte da Empresa: média
Nº de Empregados: cerca de 450
Faturamento Anual: não informado
Capital Social: não informado

Recursos Tecnológicos Disponíveis Atualmente:

• 1 servidor de arquivos – (Linux); Configuração: Intel Pentium Xeon CPU 2.70 GHz 6GB;

• 1 servidor de DNS/Internet – (Linux); Configuração: Intel Pentium Xeon CPU 2.70 GHz 6GB;

• 1 servidor de Email – (Windows Server 2008); Configuração: Intel Pentium 4 CPU 3.06 GHz 4 GB;

• 9 servidores de arquivos (Filiais) – (Linux); Configuração: Intel Pentium 4 CPU 3.06

GHz 4 GB;

Filiais:

• 75 Pentium Core2Duo 2.6 GHz 2GB;

• 20 Core I3 2.8 GHz 3GB;

Escritório Central:

• Pentium 4 Dual Core 3.0 512 MB;

• 20 Core I3 2.8 GHz 3GB;

Impressoras:

• 9 Xerox Phaser 3420;

• 12 LX 810;

Todas as filiais estão interligadas em rede e possuem acesso à Internet 24 horas por dia com *link* privativo e exclusivo de 1 MB. A estrutura de servidores é composta por roteadores, *firewall*, servidor de arquivos internos, servidor de correio eletrônico, servidor para internet nas filiais. O sistema operacional utilizados nos servidores é GNU/Linux. A manutenção dos equipamentos é realizada em três períodos sendo:

• Diariamente:
  - Manutenção de arquivos do sistema: Testado a integridade dos arquivos utilizados pelo sistema, manutenção do *link* de internet.
• Quinzenalmente:
  - Funcionalidade do *software*: Teste de operação do sistema operacional, atualização do antivírus, e atualização de programas em geral;
  - Funcionalidade do *Hardware*: Teste de operação do *hardware* básico como o mouse, teclado e monitor.
• Semestralmente:
  - Limpeza interna dos gabinetes, efetuando testes nos equipamentos e substituindo as peças com defeito. Formatação lógica dos discos rígidos e a reinstalação de todos os programas se necessário.

• Terceirizado ou Estrutura Própria:

- Os Supermercados Myatã LTDA possuem uma estrutura própria, onde praticamente todos os sistemas e serviços são realizados internamente, com exceção da manutenção de balanças que é feita por empresa especializada.

• Características da tecnologia da informação:

- Atualmente a tecnologia de informação está sendo de suma importância para o desenvolvimento da empresa. Todas as transações comerciais dependem da tecnologia da informação. Não há intenções de investimentos em tecnologia de informação, mas sim em investimentos no setor de comunicação da instituição.

6 RESULTADOS

6.1 Análise do *checklist*

Com base nos resultados obtidos através da aplicação do *checklist* baseado na norma ABNT NBR ISO/IEC 27002:2005 os seguintes dados foram observados:

Pôde-se verificar que de todos os controles estabelecidos pela norma, representado pelas 161 questões, a empresa atinge 88 controles representando aproximadamente 73% dos controles aplicáveis, sendo que 10 controles propostos não se aplicam a empresa. Parcialmente a empresa atinge 5 controles representando aproximadamente 5% e os controles não atingidos são 27 representando aproximadamente 22%.

• Analise e tratamento de riscos: atinge os objetivos.

A empresa busca avaliar os riscos que influenciam a gestão da informação e realiza esta análise periodicamente, alem de buscar o tratamento dos riscos levantados.

• Política de segurança da informação: atinge os objetivos.

Existe na empresa um documento apoiado e aprovado pela direção que contem todas as características da política de segurança e esta política possui um gestor que é responsável pela manutenção e analise periódica dos requisitos. Segundo o gestor a analise é feita mensalmente ou quando ocorra alguma mudança significativa.

• Organizando a segurança da informação: atinge parcialmente os requisitos

A direção apoia efetivamente a política de segurança em vigência, entretanto, não vê necessidade de uma consultoria externa para avalia-la. Em termos de responsabilidade pela segurança em cada área a empresa atinge o objetivo parcialmente, pois, nem todas as áreas possuem um representante, cada filial contêm um representante que responde pelo setor de TI da filial e as áreas pelas quais eles correspondem estão claramente definidas alem de suas responsabilidades.

A empresa não possui uma gestão de autorização para novos recursos, sendo que os mesmos devem passar pelo gestor de política da informação para a eventual instalação do

novo recurso.

A organização não vê necessidade da existência de um acordo de confidencialidade com terceiros, pois, existe um número mínimo de informações que navegam na parte externa da empresa. Todas as informações sigilosas e importantes à empresa trafegam dentro da rede local.

Existem diretrizes que orientam os funcionários que no caso de incidentes contra a segurança da informação a entrar em contato com o gestor da política de segurança da empresa para que o mesmo busque as autoridades necessárias.

• Partes externas: atinge os objetivos

A empresa entende que existem riscos envolvendo partes externas, os identifica e aplica os controles necessários e adequados aos acessos e manuseio da informação. Possui acordos com terceiros que tem como objetivo atender os requisitos de segurança a informação por partes externas não autorizadas.

• Gestão de ativos: não atinge nenhum dos objetivos

Os Supermercados Myatã LTDA não possui nenhum mecanismo para o inventario de seus ativos e acredita que é um processo complicado a se fazer, pois, existe um numero muito grande de ativos. O responsável pelos ativos é o gestor da segurança da informação, a direção não vê necessidade em ter uma pessoa responsável só pelos ativos já que o gestor da política é também o responsável pela instalação de novos recursos e atualizações no sistema.

Não existem regras identificadas e documentadas para o uso das informações dos ativos.

• Classificação da informação: atinge os objetivos

A empresa classifica toda a informação que chega com base em seu valor, requisitos legais, sensibilidade e criticidade. Todos os documentos e informações são centralizados na matriz podendo as filiais ter acesso às informações pelo sistema ou por requisição de documentos. Existem procedimentos adequados para o tratamento da informação com base na sua classificação.

• Segurança em recursos humanos: atinge parcialmente os objetivos

Segundo os resultados obtidos a empresa se preocupa com as diretrizes de segurança nos recursos humanos. Os papeis e as responsabilidades de colaboradores são definidas e documentadas conforme a política de segurança. O histórico de cada candidato é consultado e estabelece como obrigação contratual o comprometimento dos colaboradores com a política de segurança da informação.

Periodicamente os colaboradores recebem treinamento quanto à conscientização e atualizações na política de segurança. A empresa não possui nenhum processo disciplinar a colaboradores que cometem violações de segurança.

Quanto ao encerramento de atividades a empresa deixa clara a responsabilidade para a realização de encerramento de contrato.

• Segurança física e do ambiente: Atinge parcialmente os requisitos

Quanto às áreas de segurança a empresa utiliza perímetros para a proteção das áreas e instalações que contenham informações, estes perímetros possuem controle de acesso para assegurar que pessoas não autorizadas entrem. Existe segurança física em todas as salas e escritórios que possuem equipamentos de processamento de dados, entretanto não há nenhuma diretriz contra desastres naturais ou causados pelo homem. O trabalho em áreas seguras é controlado assim como o acesso as informações. Pontos de entrega e carregamento são controlados contra acesso não autorizado.

Os equipamentos estão localizados em áreas protegidas do meio ambiente e acessos não autorizados, possuem diretrizes contra falta de energia e comunicação. A manutenção é feita por pessoas autorizadas em intervalos regulares ou quando surja. Equipamentos fora e dentro das dependências só podem ser manuseados por pessoas autorizadas e as mídias de armazenamento reutilizáveis são totalmente apagadas em caso de descarte.

• Gerenciamento das operações e comunicações: atinge parcialmente os requisitos.

Dentro da organização toda e qualquer modificação é restrita ao gestor da política de segurança. Grande parte das tarefas e responsabilidades operacionais é do gestor.

A empresa possui recursos de processamento de dados gerenciados por terceiros, estes são avaliados semanalmente para que atendam os requisitos de funcionamento e qualquer

mudança que deva ocorrer deve ser autorizada pelo gestor da política de segurança.

Todas as modificações, novos sistemas e atualizações passam por inúmeros testes antes de serem implementados nas filiais.

Todas as máquinas da empresa possuem *software* contra códigos maliciosos, atualizados diariamente e que analisam toda a informação que trafega na rede, alem de que a rede possui um *firewall* para proteção contra acessos externos. É expressamente proibido aos colaboradores instalarem *softwares* nos equipamentos da empresa sem a autorização do responsável da filial, entretanto os equipamentos não possuem nenhum controle quanto ao uso de dispositivos móveis.

Os Supermercados Myatã LTDA realizam *backup* de seus dados diariamente em uma mídia externa a rede, que é verificada semanalmente. Existe controle do fluxo de informação na rede tanto a interna quanto a externa. A empresa se preocupa com a integridade da informação que trafega na rede, mas por se tratar de rede interna não se preocupa com confidencialidade.

As mídias removíveis são classificadas conforme sua importância para a organização, e isto decide a forma que a mesma deve ser descartada ou por vezes guardada em local seguro. Toda a informação das mídias e protegida contra acesso não autorizado e a documentação dos sistemas é restrita ao gestor e usuários autorizados.

A empresa mantém *logs* das atividades dos administradores e usuários nos sistemas, e dos controles contra acessos não autorizados, mas não vê necessidade de monitorar uso de recursos de processamento, eventos de segurança da informação e falhas ocorridas. Todos os equipamentos estão em sincronia de relógios.

• Controle de acessos: Atingiu parcialmente os objetivos

O uso dos ativos e sistemas da empresa e restrito a usuários autorizados pelo gestor de política de segurança. A autenticação é feita através de uma senha pessoal e intransferível que deva seguir boas praticas de segurança, o acesso aos módulos do sistema de controle e controlado levando em consideração a necessidade do usuário. É aconselhado aos usuários que mantenham o sistema fechado quando em inatividade.

Somente usuários autorizados tem acesso a rede seja interno ou externo. O acesso aos equipamentos de redes é restrito ao gestor da política de segurança. Existem controles de conexão para redes que se estendam aos limites da empresa e o roteamento e controlado para que o fluxo das informações não viole a política de controle de acesso.

O acesso ao sistema operacional e controlado por usuário e senha. Cada filial possui uma identificação única. A empresa não vê necessidade em controlar o tempo de inatividade dos terminais, nem limite de horário para conexões. Não existe controle contra o uso de programas que podem sobrepor os controles aplicados.

Existe um controle sobre o acesso as informações e funções do sistema especificado pelo gestor da política de segurança. Não existem controles sobre a computação móvel, pois, a empresa dispõe de todos os equipamentos necessários ao funcionamento do fluxo de trabalho. O uso de equipamentos móveis por usuários é proibido dentro da empresa.

• Aquisição, desenvolvimento e manutenção de sistemas de informação: atinge parcialmente.

Em uma mudança de sistema ou algum equipamento a empresa leva em consideração se os controles de segurança poderão ser aplicados. Os dados de processamento são validados tanto entrada como saída, entretanto não existe nenhum controle para verificar a autenticidade da informação.

A empresa não possui nenhuma política de controle criptográfico implementado. A instalação de *softwares* nos equipamentos da empresa é permita somente ao gestor e usuários autorizados, entretanto não existe nenhum controle quanto a este quesito. Códigos fonte que estão em poder da empresa são restritos ao gestor da política de segurança.

A empresa desencoraja mudanças em sistemas já instalados, quando existe a necessidade de mudanças ou atualizações são efetuados testes antes da instalação nas filiais. A empresa não desenvolve *softwares*, mas supervisiona as mudanças efetuadas pela empresa proprietária do *software* utilizado.

• Gestão de incidentes de segurança da informação: atinge parcialmente os objetivos

A direção da empresa está atenta a todos os incidentes de segurança e orienta aos colaboradores e terceiros notificar qualquer fragilidade observada. A empresa não mantém nenhum registro sobre os incidentes de segurança que aconteceram, não quantifica os custos dos incidentes.

• Gestão da continuidade do negócio: Atinge parcialmente os objetivos

A empresa identifica os eventos e o impacto que podem causar interrupções na estrutura básica para a continuidade de negócios. Esta estrutura contempla todos os requisitos de segurança da informação.

• Conformidade: Atinge os objetivos

Os sistemas de informação da empresa seguem todos os requisitos estatuários, regulamentais e contratuais e estão em conformidade com as restrições legais. Os *softwares* proprietários são fornecidos com uma licença de uso. Todas as informações pessoais de colaboradores e clientes são classificadas como confidenciais.

A direção orienta os colaboradores a não utilizar os recursos de processamento para fins não autorizados. Todos os sistemas e áreas da empresa são considerados na analise critica da segurança da informação.

6.2 Incidências

A empresa preocupa-se muito pouco com a segurança dos equipamentos de processamento de dados nas filiais, embora exista controle de acesso à informação do sistema não existe qualquer diretriz contra a instalação de programas ou mesmo acesso as informações do equipamento de processamento de dados, alguns dos equipamentos estão em locais de constante movimento de pessoas estranhas. A empresa não faz inventários de seus ativos, portanto não possui controle sobre a quantidade, localização e estado caso ocorra algum incidente. O tipo mais comum de incidência é a contaminação do ambiente por Trojan e vírus. Apesar dos controles de Internet os usuários ainda acabam clicando em links indevidos que possuem agentes maliciosos, prejudicando o ambiente.

Os funcionários não passam por um processo disciplinar quando cometem alguma violação de segurança. Quanto ao uso do sistema à empresa não cobra de seus colaboradores a alteração de suas senhas pessoais periódicamente. A empresa visa sempre instruir o funcionário de modo a mudar seu comportamento, mostrando que o não cumprimento das normas pode prejudicar os objetivos da empresa. Todos os equipamentos estão sujeitos a desastres naturais ou causados pelo homem, pois não existem diretrizes contras essas ocorrências.

6.2 Sugestões de melhorias

Com base nos incidentes relatados no capitulo anterior segue uma lista de possíveis melhorias a fim de sanar as vulnerabilidades de segurança:

- Bloqueio da área de trabalho quando a estação fica inativa, alem do registro do uso dos equipamentos por usuários e administradores através de um *login* e senha para liberar a área de trabalho.
- Elaboração de normas internas de caráter disciplinar para as ocorrências relacionadas a mau uso dos equipamentos e incidentes de segurança relacionados ao comportamento dos usuários.
- Elaboração de uma política de senhas para gerenciar possíveis vulnerabilidades dos acessos ao sistema ocasionado por senhas muito fáceis de serem burladas.
- Construção de um inventário de todos os ativos, documentado e com um gestor.
- A implementação de diretrizes contra desastres pode proteger equipamentos que contenham informações importantes à empresa.

CONCLUSÃO

Após o surgimento dos computadores e da internet o mundo nunca mais foi o mesmo. À medida que as informações e dados tem um valor inestimável para as empresas, um patrimônio, fica evidente o quanto é indispensável à segurança da informação. A proteção de seus dados a qualquer custo é uma prioridade nos planos de negócio. Na medida que novas tecnologias e soluções que prometem elevado nível de segurança e proteção surgem as organizações se conscientizam cada vez mais da importância e necessidade de protegerem seus dados.

Políticas de segurança tendem a minimizar o risco a integridade, disponibilidade e confidencialidade dos dados. É um processo de modificações continuas sempre se adaptando a melhor forma de acabar com as vulnerabilidades e reduzir o impacto dos incidentes que podem vir a acontecer. As políticas de segurança são compostas de regras baseadas em normas como proposto pela norma ABNT NBR ISO/IEC 27002:2005.

Através dela é possível aplicar todos os controles adequados referentes a todas as áreas e processos sensíveis a ataques. Tais regras só se fazem uteis com a conscientização e colaboração dos usuários.

Com o *checklist* proposto pôde-se verificar o nível de conformidade da política de segurança dos Supermercados Myatã LTDA com a norma ABNT NBR ISO/IEC 27002:2005 permitindo observar as falhas e sua correção. A total conformidade com a norma garante uma proteção eficaz das informações.

REFERÊNCIAS

ADACHI, T. **Gestão de segurança em internet banking**. São Paulo: FGV, 2004. 121p. Mestrado. Fundação Getúlio Vargas. Administração. Orientador Eduardo Henrique Diniz.

ARAÚJO, M. T.; FERREIRA, F. N. F. **Política de segurança da informação: guia prático para embalagem e implementação**. 2. ed. Rio de Janeiro: Ciência Moderna, 2006. 264p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS E TÉCNICAS - ABNT **NBR ISO/IEC 27002:2005 - Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005. 140p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT **NBR ISO/IEC 17999:2005 - Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005. 120p.

BEAL, A. **Gestão estratégica da informação**. 1. Ed. São Paulo: Atlas S.A, 2005. 144p

BELLOVIN, S. M.; CHESWICK, W. R.; RUBIN, A. D. **Firewalls e segurança na internet - repelindo o hacker ardiloso**. 2. ed. Porto Alegre: Bookman, 2005. 375p.

CARUSO, C. A. A.; STEFFEN, F. D. **Segurança em informática e de informações**. 2. ed. São Paulo: SENAC São Paulo, 1999. 368p.

CARVALHO, H.; SILVA, P. T.; TORRES, C. B. **Segurança dos sistemas de informação: gestão estratégica da segurança empresarial.** Portugal: Sociedade Brasileira de Telecomunicações, 2003. 255p.

DAWEL, George. A **Segurança da Informação nas Empresas**. Rio de Janeiro: Editora Ciência Moderna, 2005.

DIAS, C. **Segurança e auditoria da tecnologia da informação.** Rio de Janeiro: Axcel Books, 2000. 218p.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 3. Ed. Porto Alegre: Bookman, 2006. 844p.

GEUS, P. L.; NAKAMURA, E. T. **Segurança em redes em ambientes cooperativos**. São Paulo: Futura, 2003. 488p.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas S.A, 1999. 374p.

GIL, A. L. **Auditoria de Computadores**. 4. Ed. São Paulo: Atlas, 1999.

GUIMARÃES, A. G.; LINS, R. D.; OLIVEIRA, R. **Segurança com redes privadas virtuais - VPNs**. Rio de Janeiro: Brasport, 2006. 215p.

HONEYCUTT, J. **Usando a Internet**. Rio de Janeiro: Campus, 1998. 95p.

HONÓRIO, P. H. A. HACKERS Como se proteger?. 2003. Monografia (Graduação em Ciências da Computação), Centro Universitário do Triângulo, Uberlândia, 2003. Disponível em: <https://www.computacao.unitri.edu.br/downloads/monografia/28211129128857.pdf >. Acesso em: 21 Setembro. 2012.

JUNIOR, M. F. **Guia essencial do backup**. São Paulo: Digerati Books, 2007. 128p.

LAUREANO, P. A. M, **Gestão de Segurança da Informação**, [em linha] disponível em < www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf> Acesso em 15 de Outubro de 2012

KAHN, D. **História da criptologia – história antiga,** fevereiro de 2004. Disponível em: <http://www.numaboa.com.br/criptologia/historia/antiga.php> Acesso em 22 de Outubro de 2012

LAKATOS, E. M.; MARCONE, A. M. **Metodologia do trabalho científico**. 4. ed. São Paulo: Atlas S.A, 1992. 212p.

MORAES, G. D. A.; TERENCE, A. C. F.; ESCRIVÃO FILHO, E. **A tecnologia como suporte à gestão da tecnologia e sistemas de informação na pequena empresa.** In: Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação**,** 1, 21-23/06/2004, São Paulo, TECSI/FEA/USP.

REZENDE, D. A.; ABREU, A. F.; **Tecnologia da informação – aplicada a sistemas de informação empresariais.** São Paulo. 8. Ed. Atlas S.A. 2012.

SCHNEIER, B. **Segurança.com, Tradução de "Secrets & Lies", Segredos e Mentiras sobre a Proteção na Vida Digital**. Rio de Janeiro: Campus, 2001. 404p.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Campus, 2003. 184p.

STALLINGS, W. **Arquitetura e organização de computadores.** 5 Ed. Rio de Janeiro. Prentice Hall, 2002. 808p

TANENBAUM, A. S. **Computer Networks**. 4. ed. São Paulo: Campos, 2003. 632p.

WADLOW, T. **Segurança de redes**. Rio de Janeiro: Campus, 2000. 256p.

APENDICE A - CHECKLIST PARA AVALIAÇÃO DA SEGURANÇA DA INFORMAÇÃO COM BASE NA NORMA ISO/IEC 27002:2005 APLICADO NOS SUPERMERCADOS MYATÃ LTDA

Checklist para avaliação da segurança da informação com base na norma ISO/IEC 27002:2005				
Sequencia	**Padrão**	**Seção da norma**	**Questão auditoria**	**A/AP/NA**
			A= Atinge AP= Atinge parcialmente NA= Não atinge	
1.0	4.0	Analise/avaliação e tratamento de riscos		
1.1	4.1	Analisando/avaliando os riscos de segurança da informação		
1.1.1	4.1.1		Se existe uma análise/avaliação de riscos, as quais os resultados influenciem a gestão da informação.	
			Se esta é realizada periodicamente, para contemplar mudanças nos requisitos da informação e utiliza de uma forma metódica.	
1.1.2	4.1.2		Se a organização considera o tratamento dos riscos levantados durante a analise/avaliação	
2.0	5.0	Política de segurança da informação		
2.1	5.1	Política de segurança da informação		
2.1.1	5.1.1	Documento da política de segurança da informação	Se existe um documento da política de segurança da informação aprovado pela direção e comunicado para os funcionários e partes externas.	
			Se este documento contem todas as características da política de segurança da informação, suas metas e importância dentro da organização.	
2.1.2	5.1.2	Analise crítica da política de segurança da informação	Se a política da segurança possui um gestor e que este tenha a responsabilidade pela manutenção e analise critica da informação.	
			Se a análise crítica da política de segurança ocorre em decorrência de mudanças no ambiente organizacional, as circunstancias do negócio, condições legais e ambientes técnicos.	
3.0	6.0	Organizando a segurança da informação		
3.1	6.1	Organização interna		
3.1.1	6.1.1	Comprometimento da direção com a segurança da informação	Se existe apoio efetivo da direção com a segurança da informação dentro da organização, com claro direcionamento, reconhecendo as responsabilidades e demonstrando o seu comprometimento.	
			Se a direção identifica as necessidades para a consultoria de um especialista, analise criticamente e coordene os resultados desta consultoria.	
3.1.2	6.1.2	Coordenação da segurança da informação	Se as atividades referentes a segurança da informação são coordenadas por representantes de diferentes partes da empresa, com funções e papeis relevantes a informação.	
3.1.3	6.1.3	Atribuição de responsabilidades para a segurança da informação	Se todas as responsabilidades pela segurança da informação estão claramente definidas em relação a política de segurança, aos ativos, locais, recursos de processamento e a realização dos processos de segurança.	
			Se as áreas pelas quais as pessoas sejam responsáveis estão claramente definidas.	
3.1.4	6.1.4	Processo de autorização para os	Se existe definido e implementado um processo de gestão de autorização para novos recursos de processamento da	

		recursos de processamento da informação	informação incluindo os softwares e hardwares.	
3.1.5	6.1.5	Acordos de confidencialidade	Se existem acordos de confidencialidade ou não divulgação que considerem os requisitos de proteção de informação confidencial em conformidade com todas as leis e regulamentações aplicáveis.	
3.1.6	6.1.6	Contato com autoridades	Se a organização possui procedimentos que especifiquem com quais autoridades e quando devem ser contatadas em caso de incidentes na segurança da informação.	
3.1.7	6.1.7	Contato com grupos especiais	Se existe contato com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações especializadas.	
3.1.8	6.1.8	Analise critica independente da segurança da informação	Se o enfoque da organização para gerenciar a segurança da informação e sua implementação e analisado criticamente de forma independente periodicamente ou quando ocorrem mudanças significativas.	
3.2	6.2	Partes externas		
3.2.1	6.2.1	Identificação dos riscos relacionados com partes externas	Se os riscos que envolvem partes externas são identificados e os controles aplicados antes de conceder o acesso às informações.	
			Se os tipos de acesso são identificados, classificados e as razoes justificadas.	
3.2.2	6.2.2	Identificando a segurança da informação quando tratando com os clientes	Se todos os requisitos de segurança da informação são identificados antes de conceder acesso aos clientes as informações da organização.	
3.2.3	6.2.3	Identificando a segurança da informação nos acordos com terceiros	Se existe um acordo com terceiros que cubra todos os requisitos de segurança da informação relevantes identificando os porquês, meios e justificativas.	
4.0	7.0	Gestão de ativos		
4.1	7.1	Responsabilidade pelos ativos		
4.1.1	7.1.1	Inventário dos ativos	Se todos os ativos da organização são identificados e exista um inventário de todos os ativos estruturado e mantido	
4.1.2	7.1.2	Proprietário dos ativos	Se existe um gestor para as informações e ativos associados com os recursos de processamento da informação que analise criticamente as classificações e restrições ao acesso	
4.1.3	7.1.3	Uso aceitável dos ativos	Se existem regras identificadas, documentadas e implementadas permitindo o uso de informações e ativos.	
4.2	7.2	Classificação da informação		
4.2.1	7.2.1	Recomendações para classificação	Se toda a informação e classificada levando em consideração o seu valor, requisitos legais, sensibilidade e criticidade.	
4.2.2	7.2.2	Rótulos e tratamento da informação	Se um conjunto apropriado de procedimentos foi definido para rotular e tratar a informação de acordo com o esquema de classificação adotado pela organização	
5.0	8.0	Segurança em recursos humanos		
5.1	8.1	Antes da contratação		
5.1.1	8.1.1	Papéis e responsabilidades	Se os papeis e responsabilidades de funcionários, fornecedores e terceiros pela segurança da informação são definidos e documentados de acordo com a política	

			de segurança.	
5.1.2	8.1.2	Seleção	Se forem realizadas verificações do histórico de todos os candidatos a emprego, fornecedores e terceiros, de acordo com a ética e as regulamentações pertinentes e proporcionais aos requisitos do negocio.	
5.1.3	8.1.3	Termos e condições de contratação	Se os funcionários, fornecedores e terceiros são questionados a declarar como parte de suas obrigações contratuais sua responsabilidade e a da organização para a segurança da informação.	
5.2	8.2	Durante a contratação		
5.2.1	8.2.1	Responsabilidades da direção	Se a direção solicita aos colaboradores que pratiquem a segurança da informação de acordo com as políticas e procedimentos da organização	
5.2.2	8.2.2	Conscientização, educação e treinamento em segurança da informação.	Se os colaboradores recebem treinamento apropriado quanto à conscientização e atualizações nas políticas de segurança e procedimentos organizacionais relevantes.	
5.2.3	8.2.3	Processo disciplinar	Se existe um processo disciplinar aos funcionários que tenham cometido violação da segurança da informação levando em consideração a gravidade e natureza.	
5.3	8.3	Encerramento ou mudança de contrato		
5.3.1	8.3.1	Encerramento de atividades	Se as responsabilidades para realizar o encerramento ou a mudança de um trabalho sejam claramente definidas e atribuídas.	
5.3.2	8.3.2	Devolução de ativos	Se a política da empresa exige a devolução de todos os ativos da organização que estejam em posse de colaboradores após o encerramento de atividades, do contrato ou acordo.	
5.3.3	8.3.3	Retirada de direitos de acesso	Se os direitos de acesso dos colaboradores aos recursos de processamento da informação são retirados após o encerramento de suas atividades, contratos, acordos ou ajustados após a mudança de função.	
6.0	9.0	Segurança física e do ambiente		
6.1	9.1	Áreas seguras		
6.1.1	9.1.1	Perímetro da segurança física	Se forem utilizados perímetros de segurança tais como paredes, portões controlados por cartão ou recepção com recepcionista para proteger as áreas que contenham informações e instalações do processamento de informações.	
6.1.2	9.1.2	Controles de entrada física	Se existem controles de entrada física para assegurar que pessoas não autorizadas tenham acesso as áreas seguras.	
6.1.3	9.1.3	Segurança em escritórios, salas e instalações.	Se a segurança física esta aplicada em salas, escritórios e instalações onde existam equipamentos de processamento de dados.	
6.1.4	9.1.4	Proteção contra ameaças externas e do meio ambiente	Se existem diretrizes de segurança física projetada e aplicada contra incêndios, enchentes, terremotos, explosões, perturbações da ordem ou outras formas de desastres naturais ou causados pelo homem.	
6.1.5	9.1.5	Trabalhando em áreas seguras	Se existe algum controle para o trabalho em áreas seguras onde a informação só é divulgada a quem seja necessário e quando for necessário.	
6.1.6	9.1.6	Acesso ao publico, áreas de entrega e de carregamento.	Se os pontos de acesso a áreas de entrega e carregamento são controlados contra acesso não autorizado a áreas do processamento da informação	
6.2	9.2	Segurança de equipamentos		

6.2.1	9.2.1	Instalação e proteção do equipamento	Se os equipamentos de processamento da informação estão em áreas protegidas dos perigos do meio ambiente e acessos não autorizados.	
6.2.2	9.2.2	Utilidades	Se for aplicado às áreas de processamento de dados diretrizes contra falta de energia ou eventuais falhas em outras utilidades.	
6.2.3	9.2.3	Segurança do cabeamento	Se o cabeamento de energia e comunicações de dados esta protegido de alguma forma contra interrupções ou danos	
6.2.4	9.2.4	Manutenção dos equipamentos	Se a manutenção em equipamentos de processamento de dados é feita por pessoas autorizadas e em intervalos regulares de acordo com as suas especificações.	
6.2.5	9.2.5	Segurança de equipamentos fora das dependências da organização	Se existem medidas de segurança para equipamentos fora das dependências da organização levando em conta os diferentes riscos de se trabalhar fora do perímetro de segurança.	
6.2.6	9.2.6	Reutilização e alienação segura de equipamentos	Se os equipamentos contem mídias de armazenamento reutilizáveis assegurando que no caso de descarte as informações sensíveis sejam removidas ou sobregravados.	
6.2.7	9.2.7	Remoção de propriedade	Se existem controles contra a remoção não autorizada de equipamentos, informações ou softwares.	
7.0	10.0	Gerenciamento das operações e comunicações		
7.1	10.1	Procedimentos e responsabilidades operacionais		
7.1.1	10.1.1	Documentação dos procedimentos de operação	Se todos os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.	
7.1.2	10.1.2	Gestão de mudanças	Se existem diretrizes de controle sobre modificações nos recursos de processamento da informação e sistemas.	
7.1.3	10.1.3	Segregação de funções	Se as tarefas e áreas de responsabilidades são separadas para reduzir a possibilidade de modificação não autorizada ou mal uso de informações ou serviços.	
7.1.4	10.1.4	Separação dos recursos de desenvolvimento, teste e de produção.	Se os recursos de desenvolvimento, teste e produção são separados para reduzir o risco de acessos ou modificações não autorizadas.	
7.2	10.2	Gerenciamento de serviços terceirizados		
7.2.1	10.2.1	Entrega de serviços	Se existe algum recurso de processamento gerenciado por terceiros e que sejam implementados, executados e mantidos por terceiros.	
7.2.2	10.2.2	Monitoramento e analise critica de serviços terceirizados	Se for efetuada alguma auditoria critica regularmente sobre os serviços, relatórios e registros fornecidos por terceiros e se os mesmos são monitorados.	
7.2.3	10.2.3	Gerenciamento de mudanças para serviços terceirizados	Se as mudanças em contratos com terceiros são gerenciados levando em consideração a criticidade dos sistemas e processos de negócio envolvidos e a reanalise/reavaliação de riscos.	
7.3	10.3	Planejamento e aceitação dos sistemas		
7.3.1	10.3.1	Gestão de capacidade	Se existem controles da utilização dos recursos de processamento da informação e projeções de necessidades futuras.	
7.3.2	10.3.2	Aceitação de sistemas	Se existem critérios de aceitação para novos sistemas, atualizações e novas versões e se são realizados testes nos mesmos.	
7.4	10.4	Proteção contra códigos maliciosos		
7.4.1	10.4.1	Controles contra	Se existe algum controle contra o uso de softwares	

		códigos maliciosos	maliciosos	
			Se existe uma política contra o uso de software não autorizado	
			Se existe algum software de detecção e remoção de códigos maliciosos instalado nos equipamentos da organização	
			Se estes softwares para detecção e remoção estão com a assinatura e seu banco de dados atualizado para a detecção de vírus	
			Se todo o trafego que possa conter código malicioso e analisado por estes softwares de detecção e remoção	
7.4.2	10.4.2	Controle contra códigos móveis	Se existem algum controle contra o uso de equipamentos de armazenamento móvel dentro dos equipamentos da empresa.	
7.5	10.5	Cópias de Segurança		
7.5.1	10.5.1	Cópias de segurança da informação	Se existe algum mecanismo para efetuar copias de segurança das informações da organização realizado regularmente	
			Se a mídia que contem a copia de segurança e o meio para restaurá-la são guardados em locais separados do local onde foram realizados	
			Se a mídia e regularmente verificada e a integridade dos dados testada	
7.6	10.6	Gerenciamento da segurança em redes		
7.6.1	10.6.1	Controle de redes	Se existe algum controle do fluxo de informações na rede	
			Se a responsabilidade operacional e procedimentos sobre o gerenciamento de equipamentos remotos foi estabelecido	
			Se existe algum controle para garantir a integridade e confidencialidade da informação que trafega na rede.	
7.6.2	10.6.2	Segurança nos serviços de rede	Se existe algum acordo com terceiros sobre serviços de rede e que este inclua as características da segurança, níveis de serviço e requisitos de gerenciamento dos serviços da rede.	
7.7	10.7	Manuseio de mídias		
7.7.1	10.7.1	Gerenciamento de mídias removíveis	Se existe algum procedimento para o gerenciamento de mídias removíveis	
7.7.2	10.7.2	Descarte de mídias	Se as mídias que perderam sua utilidade são descartadas de forma segura e protegida	
			Se os itens sensíveis são registrados em controles quando é feito o descarte, para manter uma trilha de auditoria.	
7.7.3	10.7.3	Procedimentos para tratamento de informação	Se existe algum procedimento para o tratamento e armazenamento de informações. Este define o tratamento e identificação bem como proteção contra mau uso da informação e uso não autorizado	
7.7.4	10.7.4	Segurança da documentação dos sistemas	Se existe algum tipo de controle ao acesso da documentação dos sistemas	
7.8	10.8	Troca de informações		
7.8.1	10.8.1	Políticas e procedimentos para troca de informações	Se existem procedimentos, políticas e controles estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação da organização.	
7.8.2	10.8.2	Acordos para troca de informações	Se existem acordos para a troca de informações entre a organização e entidades externas	

			Se estes acordos definem as características da segurança baseadas na sensibilidade das informações de negocio envolvidas.	
7.8.3	10.8.3	Mídias em transito	Se existe proteções contra alteração, uso não autorizado ou uso impróprio durante o transporte externo aos limites físicos da organização.	
7.8.4	10.8.4	Mensagens eletrônicas	Se existe algum procedimento para a proteção de informações que trafegam em mensagens eletrônicas.	
7.8.5	10.8.5	Sistemas de informações do negocio	Se existem diretrizes ativas para proteger as informações associadas com a interconexão de informações do negocio.	
7.9	10.9	Serviços de comercio eletrônico		
7.9.1	10.9.1	Comercio eletrônico	Se o comercio eletrônico e bem protegido e se controles foram implementados para a proteção contra atividades fraudulentas, disputa de contrato, exposição ou modificação das informações.	
7.9.2	10.9.2	Transações on-line	Se existe controles para proteger a informação em transações on-line	
7.9.3	10.9.3	Informações publicamente disponíveis	Se existe alguma diretriz para prevenir modificações não autorizadas em sistemas publicamente acessíveis.	
7.10	10.10	Monitoramento		
7.10.1	10.10.1	Registro de auditoria	Se existem registros de atividades dos usuários, exceções e outros eventos de segurança da informação.	
			Se estes registros produzidos são mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento do controle de acessos.	
7.7.2	10.10.2	Monitoramento do uso do sistema	Se existe registro do uso dos recursos de processamento da informação	
			Se os resultados destes registros e monitoração são analisados criticamente regularmente	
7.7.3	10.10.3	Proteção das informações dos registros (logs)	Se existem controles contra acesso não autorizado e alterações as informações de registro (logs)	
7.7.4	10.10.4	Registros de administrador e operador	Se os registros de acesso contem as atividades dos administradores e operadores do sistema.	
7.7.5	10.10.5	Registros de falhas	Se existem registros das falhas ocorridas	
			Se estes registros são analisados criticamente e que sejam adotadas as ações apropriadas.	
7.7.6	10.10.6	Sincronização dos relógios	Se todos os relógios dos sistemas de processamento da informação relevantes estão sincronizados por uma fonte de tempo precisa, acordada.	
8.0	11.0	Controle de acessos		
8.1	11.1	Requisitos de negocio para controle de acesso		
8.1	11.1.1	Política de controle de acessos	Se existe uma política de controle de acessos dos sistemas e ativos da informação	
			Se a política de controle de acesso define as regras e direitos para cada usuário ou um grupo de usuários	
8.2	11.2	Gerenciamento do usuário		
8.2.1	11.2.1	Registro do usuário	Se existem procedimentos formais de registro e cancelamento de usuários para garantir e revogar acesso em todos os sistemas de informação e serviços	
8.2.2	11.2.2	Gerenciamento de privilégios	Se a concessão e o uso de privilégios é restrito e controlado levando em consideração a necessidade de	

			acesso do usuário	
8.2.3	11.2.3	Gerenciamento de senha do usuário	Se existe um processo formal para o gerenciamento de concessão de senhas e alteração	
8.2.4	11.2.4	Analise critica dos direitos de acesso do usuário	Se for feita uma analise critica a intervalos regulares dos diretos de acessos dos usuários	
8.3	11.3	Responsabilidade dos usuários		
8.3.1	11.3.1	Uso de senhas	Se e solicitado aos usuários seguir boas praticas de segurança na escolha e uso de senhas.	
			Se o usuário é solicitado a assinar uma declaração de confidencialidade de sua senha pessoal	
8.3.2	11.3.2	Equipamentos de usuários sem monitoração	Se os usuários e prestadores de serviços são avisados dos requisitos de segurança e procedimentos para proteger equipamentos sem monitoração, assim como suas responsabilidades. Ex: logoff quando a seção dor finalizada.	
8.3.3	11.3.3.	Política de mesa limpa e tela limpa	Se a empresa adota uma política de mesa limpa de papeis e mídias de armazenamento removível e política de tela limpa para os recursos de processamento da informação. Ex: papeis e mídias importantes são guardadas em locais seguros quando não em uso e computadores e equipamentos desligados ou protegidos por mecanismos de travamento.	
8.4	11.4	Controle de acesso à rede		
8.4.1	11.4.1	Política de uso dos serviços de rede	Se existem políticas de controle onde os usuários só tenham acesso para os serviços de rede que tenham sido especificamente autorizados a usar	
8.4.2	11.4.2	Autenticação para conexão externa do usuário	Se existe algum mecanismo de autenticação para conexões externas.	
8.4.3	11.4.3	Identificação do equipamento em rede	Se as identificações automáticas de equipamentos é considerada como meio de autenticar conexões vindas de localizações e equipamentos específicos	
8.4.4	11.4.4	Proteção de portas de configuração e diagnósticos remotos	Se o acesso físico e lógico a portas de diagnostico e configuração dos equipamentos de rede é controlado	
8.4.5	11.4.5	Segregação de redes	Se a rede onde colaboradores e terceiros tenham acesso é segregada usando mecanismos de segurança de perímetros como firewall	
8.4.6	11.4.6	Controle de conexão de rede	Se existe algum controle de conexão de redes para redes compartilhadas que se estendem aos limites da empresa	
8.4.7	11.4.7	Controle de roteamento de redes	Se existem controles do roteamento na rede para assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negocio.	
8.5	11.5	Controle de acesso ao sistema operacional		
8.5.1	11.5.1	Procedimentos seguros de entrada no sistema (log-on)	Se existem procedimentos de controle seguro de entrada no sistema no acesso ao sistema operacional. Este procedimento deve ser projetado para minimizar a possibilidade de acessos não autorizados.	
8.5.2	11.5.2	Identificação e autenticação do usuário	Se todos os usuários possuem uma identificação única para uso pessoal e exclusivo.	
			Se o método de autenticação seja uma técnica adequada para validar a identidade de um usuário.	
8.5.3	11.5.3	Sistema de gerenciamento de	Se existe um sistema de gerenciamento de senhas interativo e assegure os vários controles de qualidade de	

		senha	senhas	
8.5.4	11.5.4	Uso de utilitários de sistema	Se existe algum controle para o uso de programas utilitários que podem sobrepor os controles do sistema e aplicações	
8.5.5	11.5.5	Limite de tempo de sessão	Se as sessões e terminais inativos são configurados para limpara a tela ou encerrar após um período de tempo.	
8.5.6	11.5.6	Limitação do horário de conexão	Se existe alguma restrição nos horários de conexão utilizada para proporcionar segurança adicional para aplicações de alto risco	
8.6	11.6	Controle de acesso à aplicação e a informação		
8.6.1	11.6.1	Restrição de acesso à informação	Se existem diretrizes para o controle do acesso a informação e as funções dos sistemas de aplicação por usuários e pessoal do suporte de acordo com o definido na política de segurança da informação	
8.6.2	11.6.2.	Isolamento dos sistemas sensíveis	Se sistemas sensíveis são isolados do ambiente de computação como sendo executados em computação dedicada	
8.7	11.7	Computação móvel e trabalho remoto		
8.7.1	11.7.1	Computação e comunicação móvel	Se existe uma política formal estabelecida com medidas de segurança apropriadas para a proteção contra riscos da computação e comunicação móvel	
8.7.2	11.7.2	Trabalho remoto	Se existe alguma política, procedimento para controle das atividades de trabalho remoto.	
			Se a proteção apropriada para o local do trabalho remoto foi implantada	
9.0	12.0	Aquisição, desenvolvimento e manutenção de sistemas de informação.		
9.1	12.1	Requisitos de segurança de sistemas de informação		
9.1.1	12.1.1	Analise e especificação dos requisitos de segurança	Se os requisitos para controles de segurança são especificados nos requisitos de negócio para novos sistemas de informação ou melhorias nos sistemas existentes.	
9.2	12.2	Processamento correto nas aplicações		
9.2.1	12.2.1	Validação dos dados de entrada	Se os dados de entrada das aplicações são verificados e validades para garantir que são corretos e apropriados	
9.2.2	12.2.2	Controle do processamento interno	Se áreas de risco são identificadas no ciclo de processamento e que checagens de validação foram incluídas	
			Se controles apropriados são identificados para aplicações a fim de minimizar os riscos durante o processamento interno	
9.2.3	12.2.3	Integridade das mensagens	Se os controles apropriados são identificados e implementados para garantir a autenticidade e proteger a integridade das mensagens em aplicações	
9.2.4	12.2.4	Validação dos dados de saída	Se os dados de saída das aplicações são validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstancias.	
9.3	12.3	Controles criptográficos		
9.3.1	12.3.1	Política para o uso de controles criptográficos	Se existe uma política implementada para o uso de controles de criptografia para a proteção da informação	
			Se for feita uma analise para identificar qual o nível de proteção dos dados	
9.3.2	12.3.2	Gerenciamento de chaves	Se existe um processo de gerenciamento de chaves implantado para apoiar o uso de técnicas criptográficas	
9.4	12.4	Segurança dos arquivos do sistema		

9.4.1	12.4.1	Controle de software operacional	Se existem controles para a instalação de software em sistemas operacionais implantados para proteção contra instalações não autorizadas	
9.4.2	12.4.2	Proteção dos dados para teste de sistema	Se existem diretrizes de controle para que os dados de teste sejam selecionados com cuidado e protegidos	
9.4.3	12.4.3	Controle de acesso ao código fonte de programas	Se o código fonte dos sistemas é restrito aos administradores e usuários autorizados	
9.5	12.5	Segurança em processos de desenvolvimento e de suporte		
9.5.1	12.5.1	Procedimentos para controle de mudanças	Se a implementação de mudanças nos sistemas e ativos é controlado por procedimentos formais	
9.5.2	12.5.2	Analise critica das aplicações após mudanças no sistema operacional	Se forem executados testes quando sistemas operacionais são mudados para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança	
			Se as aplicações criticas de negócios são analisadas criticamente para assegurar que não foram comprometidas pelas mudanças	
9.5.3	12.5.3	Restrições sobre mudanças em pacotes de software	Se a organização desencoraja mudanças em pacotes de software limitadas as mudanças necessárias e sejam estritamente controlados	
9.5.4	12.5.4	Vazamento de informações	Se existem diretrizes para prevenir o vazamento de informações da organização.	
9.5.5	12.5.5	Desenvolvimento terceirizado do software	Se a organização supervisiona o desenvolvimento terceirizado do software utilizado.	
9.6	12.6	Gestão de vulnerabilidades técnicas		
9.6.1	12.6.1	Controle de vulnerabilidades técnicas	Se existe algum procedimento para a obtenção de informações em tempo hábil sobre vulnerabilidades técnicas dos sistemas em uso e avaliando a exposição a estas vulnerabilidades	
			Se forem tomadas as medidas apropriadas para lidar com os riscos associados a estas vulnerabilidades	
10.0	13.0	Gestão de incidentes de segurança da informação		
10.1	13.1	Notificação de fragilidades e eventos de segurança da informação		
10.1.1	13.1.1	Notificação de eventos de segurança da informação	Se a direção é informada sobre todos os eventos de segurança da informação através dos canais apropriados	
10.1.2	13.1.2	Notificando fragilidades de segurança da informação	Se a organização orienta os funcionários, fornecedores e terceiros a registrar e notificar qualquer observação ou suspeita de fragilidades em sistemas e serviços.	
10.2	13.2	Gestão de incidentes de segurança da informação e melhorias		
10.2.1	13.2.1	Responsabilidades e procedimentos	Se a organização estabelece as responsabilidades e procedimentos de gestão para assegurar respostas rápidas efetivas e ordenadas a incidentes de segurança da informação	
10.2.2	13.2.2	Aprendendo com os incidentes de segurança da informação	Se a organização estabelece mecanismos para quantificar e monitorar as quantidades e custos dos incidentes de segurança	
10.2.3	13.2.3	Coleta de evidencias	Se a organização retém possíveis informações nos casos de uma ação de acompanhamento contra uma pessoa ou organização e apresentadas em conformidade com as normas de armazenamento de evidencias	

11.0	14.0	Gestão de continuidade do negócio		
11.1	14.1	Aspectos da gestão de continuidade do negócio, relativos a segurança da informação		
11.1.1	14.1.1	Incluindo segurança da informação no processo de gestão da continuidade do negócio	Se for implantado um processo de gerenciamento que permeia toda a organização para desenvolvimento e manutenção da continuidade do negócio	
11.1.2	14.1.2	Continuidade de negócios e analise/avaliação de riscos	Se eventos que podem causar interrupções aos processos de negócio foram identificados	
			Se for identificado os riscos e impacto de tais interrupções no processo de negócio	
11.1.3	14.1.3	Desenvolvimento e implementação de planos de continuidade relativos a segurança da informação	Se um plano estratégico foi desenvolvido para determinar uma aproximação global da continuidade do negócio	
11.1.4	14.1.4	Estrutura do plano de continuidade do negócio	Se existe uma estrutura básica para a continuidade dos negócios	
			Se esta estrutura contempla todos os requisitos de segurança da informação e identifica prioridades para testes e manutenção	
11.1.5	14.1.5	Testes, manutenção e reavaliação dos planos de continuidade do negocio.	Se os planos de continuidade de negócios são testados e atualizados regularmente de forma a assegurar sua permanente atualização e efetividade	
12.0	15.0	Conformidade		
12.1	15.1	Conformidade da legislação aplicável		
12.1.1	15.1.1	Identificação da legislação aplicável	Se todos os requisitos regulamentais, estatuários e contratuais pertinentes estão definidos, documentados e atualizados para cada sistema de informação	
12.1.2	15.1.2	Direitos de propriedades intelectuais	Se existe algum procedimento para assegurar conformidade com as restrições legais no uso de material de acordo com as leis de propriedade intelectual.	
			Se produtos de software proprietário são fornecidos sob um contrato de licenciamento	
12.1.3	15.1.3	Proteção de registros organizacionais	Se a organização protege os registros importantes contra perda, destruição e falsificação de acordo com os requisitos regulamentares, estatuários, contratuais e do negócio.	
12.1.4	15.1.4	Proteção de dados e privacidade de informações pessoais	Se for implantada uma estrutura de gerenciamento e controle para proteger dados e a privacidade da informação pessoal	
12.1.5	15.1.5	Prevenção do mau uso de recursos de informação	Se a organização orienta os usuários a não usar os recursos de processamento da informação para propósitos não autorizados	
12.1.6	15.1.6	Regulamentação de controles de criptografia	Se a regulamentação de controles da criptografia esta legal com os acordos locais e nacionais	
12.2	15.2	Conformidade com normas e políticas de segurança da informação e conformidade técnica		
12.2.1	15.2.1	Conformidade com as políticas e normas de segurança da informação	Se todas as áreas da empresa sejam consideradas na analise critica da segurança da informação para garantir a conformidade com as normas e políticas de segurança	

12.2.2	15.2.2	Verificação da conformidade técnica	Se todos os sistemas de informação sejam consideradas na analise critica da segurança da informação para garantir a conformidade com as normas e políticas de segurança	
12.3	15.3	Considerações quanto à auditoria de sistemas de informação		
12.3.1	15.3.1	Controles quanto à auditoria de sistemas de informação	Se a organização planeja cuidadosamente os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais para minimizar riscos de interrupção nos processos do negócio.	
12.3.2	15.3.2	Proteção de ferramentas de auditoria de sistemas de informação	Se a organização protege o acesso as ferramentas de auditoria de sistemas da informação para prevenir qualquer possibilidade de uso impróprio ou comprometimento.	
Assinatura responsável:				

Apêndice A
Fonte: Autoria própria.