Proposta de Guia de Boas Práticas de Segurança da Informação como base inicial da Política de Segurança de uma Empresa da Região do Cariri

Antônio de Pádua Pereira Carvalho

paduacarvalho@gmail.com

Abstract. *The fact that business firms are intricately connected to the computer information systems makes your digital asset to be constantly at risk. Thus, the information becomes precious and therefore must be accessible, but simultaneously safe. How to protect this information against misuse is what has been the great problem of companies seeking to keep their business on the world wide web. This work studies the area of Information Security in a company's from Cariri. Based on ISO27002 modifications were proposed to correct the nonconformities. Moreover, a good practice guide will assist in the maintenance of these corrections, thus allowing the company to develop its security policy on secure foundations. Although not corrected all the problems of security, the organization was made aware of the importance of adopting an effective security policy.*

Keywords: Security Policy, ISO 27002, Information Security

Resumo. *O fato do negócio das empresas estarem intrinsicamente ligados aos sistemas de informação computacionais faz com que o seu ativo digital esteja constantemente em risco. Desta forma, a informação se torna algo precioso e, portanto, precisa estar acessível, mas ao mesmo tempo em segurança. Como proteger essa informação contra o uso indevido é o que tem sido a grande problemática das empresas que visam manter seus negócios pela rede mundial de computadores. Este trabalho estuda a área de Segurança da Informação em uma empresa da região do Cariri. Com base na ISO27002 são propostas modificações a fim de corrigir as não conformidades encontradas. Além disso, um guia de boas práticas auxiliará na manutenção destas correções, permitindo então que a empresa elabore sua política de segurança sobre bases seguras. Embora não tenham sido corrigidos todos os problemas de segurança, a organização foi conscientizada da importância de adoção de uma politica de segurança eficaz.*

Palavras-chave: política de segurança, ISO 27002, segurança da informação

1. Introdução

A Tecnologia da informação torna-se a cada dia de extrema importância na execução dos negócios das organizações contemporâneas, sendo assim cresce exponencialmente a concorrência no mercado cibernético onde a informação é a matéria prima destas entidades, gerando assim uma problemática que merece ser discutida, a segurança da informação.

Este trabalho faz um estudo sobre normas e procedimentos a fim de verificar quais pontos podem ser melhorados quanto ao uso das informações contidas em redes de ambientes corporativos e seus recursos. Atualmente a área de Tecnologia da Informação (TI) da empresa em estudo não possui uma política de segurança. A ideia então é o desenvolvimento de um Guia estruturado na ISO 27002 que servirá como base para a política de segurança da organização.

1.1 Problema

Com o surgimento da Internet, as empresas vêm investindo em diversas tecnologias para poder ampliar o seu poder de negócio e diversificar seu contato com o seu cliente. Usar uma informação em ambiente computacional implica proporcionalmente em riscos, descoberta de vulnerabilidades e ameaças que mais tarde podem ocasionar problemas para a organização (NAKAMURA; GEUS, 2007).

Segundo Mitnick e Simon (2003, p.52), "[...] A empresa que não se esforça para proteger suas informações confidenciais é simplesmente negligente [...]". Essas empresas que não buscam proteger a informação podem estar correndo um sério risco.

Para Nakamura e Geus (2007) os riscos rondam as organizações e ocorrem quando elas oferecem algum serviço. Os atacantes têm propósitos distintos podendo gerar um problema para a organização.

1.2. Justificativa

Dada essa nova vertente tecnológica das empresas utilizando a internet como ferramenta de negocio, tem-se principalmente nesse ambiente, a necessidade de proteger informações, onde técnicas de fraudes de informação se proliferam colocando em risco a segurança.

Tais proteções e métodos precisam sempre ser aprimorados, pois frequentemente ocorrem situações inusitadas de ataques, descoberta de vulnerabilidades e novas técnicas de engenharia social, o que nos remete a uma discussão sobre políticas de segurança, em especial, a de proteção da informação e o meio em que ela é trafegada, ou seja, a infraestrutura de TI.

2. Objetivos

2.1. Objetivo Geral

Estudar e analisar a estrutura de TI da organização e apresentar uma proposta de melhoria baseado na ISO 27002 através de um guia de boas práticas, manter essas condições o qual servirá como base para a elaboração da Política de Segurança da empresa.

2.2. Objetivos Específicos

Como objetivos específicos designam-se os seguintes:

- Estudar a ISO 27002;
- Fazer um estudo sobre infraestrutura de TI e do ambiente corporativo;
- Discutir sobre a importância da implantação de políticas de segurança de redes nas organizações;
- Levantar pontos críticos da organização;
- Definir os problemas e riscos;
- Construir a proposta de implantação;
- Elaborar o guia de boas práticas.

3. Levantamento Bibliográfico

3.1. Segurança da Informação

A informação é um ativo que é essencial para os negócios de uma organização e necessita ser protegida. A segurança da informação é obtida a partir da implementação e conjunto de práticas e funções de software e hardware melhorando onde é necessário para garantir que os objetivos do negócio e de segurança da organização sejam atendidos (ABNT NBR ISO/IEC 27002).

A segurança da informação deve levar em consideração aspectos humanos e processuais de uma organização como afirma Nakamura e Geus (2007, p.45):

> A segurança de redes, assim, é uma parte essencial para a proteção da informação, porém uma boa estratégia que deve ser levada em consideração são os aspectos humanos e processuais de uma organização. Isso é importante porque outros métodos de ataque, além dos tecnológicos, afetam os níveis de segurança de uma organização.

Requisitos Básicos

De acordo com Casanas e Machado (2001) e Bauer (2006) a segurança da informação deve atender requisitos básicos como:

1. Confidencialidade: A informação pode ser acessada apenas por quem tem autorização;
2. Integridade: Certeza da precisão e da qualidade da informação;
3. Disponibilidade: Garante que os usuários autorizados tenham acesso a informação e aos recursos associados, quando necessário.

Além desses 3 pilares, outro requisito a ser considerado, segundo Souza (2004) e o Serviço Federal de Processamento de Dados (SERPRO), o Não Repúdio evita que alguma das partes envolvida na comunicação negue o envio ou recebimento de alguma informação, cuja definição – "Não-repúdio: garantia de que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica não poderá, posteriormente negar sua autoria" – encontra-se no site do SERPRO (SERPRO, 2011). Um exemplo disso é: uma empresa que autoriza uma entidade a comprar uma propriedade e depois nega que autorizou tal negociação.

Como exemplo destes requisitos tem-se uma situação real onde se pode verificar a importância das mesmas. João deseja utilizar os serviços oferecidos via Internet por seu banco. As seguintes dúvidas podem ser colocadas: a certeza de que João está

dialogando com seu banco e não com alguém que se faz passar por ele (Autenticação); a certeza de que as informações enviadas por ele ao banco e as enviadas do banco para ele são originais, ou seja, não foram alteradas durante a transmissão (Integridade); como impedir que alguém tenha acesso às informações transmitidas (Sigilo); e como o banco pode garantir-se de que, posteriormente, João venha a afirmar que não foi ele quem fez o acesso (Não-repúdio). Abaixo, outro exemplo de utilização:

Ao utilizar um serviço na internet, podemos ter a certeza que este é realmente o solicitado e que após tal transação nenhuma das partes possa negar que solicitou tal operação (SERPRO, 2011).

Alguns fatores podem comprometer a segurança da informação e precisa ser definido pela organização o grau de impacto e o prejuízo da parada de algum serviço. Entre esses temos ameaças, riscos e vulnerabilidades que será tratado em seguida.

A ISO 27002 é um código de boas práticas de segurança da informação que auxilia qualquer organização independente de sua atuação a manter seus recursos tecnológicos garantindo que seu principal ativo estará livre de qualquer meio que comprometa seu bom funcionamento.

3.1.1. Ameaças

A ameaça é um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tem uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação (ABNT NBR ISO/IEC 13335-1:2004).

O termo genérico usado para identificar quem realiza um ataque a um sistema computacional é o *hacker*. Essa generalização tem diversas ramificações, pois os ataques apresentam objetivos distintos e seu sucesso ou insucesso depende do grau de segurança e a capacidade do hacker em executá-lo (NAKAMURA; GEUS, 2007).

3.1.2. Riscos

De acordo com a ISO 27002 convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para a sua aceitação. Os resultados orientam e determinam as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos.

3.1.3. Vulnerabilidades

De acordo com Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2006), a vulnerabilidade no contexto da tecnologia da informação é definida como falha no projeto, implementação ou configuração de um software ou sistema operacional onde um *hacker*, resultando na violação da segurança de um computador ou rede de computadores.

Algumas vulnerabilidades não decorrem diretamente de má configuração ou falha de Sistema Operacional, mas são causadas devido a algum descuido ou imprudência por parte dos usuários de algum recurso como e-mail, internet ou instalação de softwares não confiáveis, propagando vírus, spywares, trojan-horses entre outros softwares maliciosos (BAUER, 2006).

3.2. Normas da Segurança da Informação

A ISO 27000 é um grupo de normas que tratam de temas relacionados à segurança da informação, sendo que esta série tem normas e documentos particulares. Entre estes estão:

- ISO 27001

A ISO/IEC 27001 é um padrão de gerenciamento de segurança da informação *(ISMS – Information Security Managemente System)* publicado em outubro de 2005 pela Associação Brasileira de Normas Técnicas (ABNT) como NBR ISO/IEC 27001. Seu nome completo é ISO/IEC 27001:2005 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gerenciamento, e trata de normas e procedimentos para gestão de informação. Este padrão foi o primeiro do grupo de segurança da informação relacionados com a série 27000 (THE ISO 27000 DIRECTORY, 2011).

Este manual cobre todos os tipos de organizações e especifica os requisitos para estabelecer, programar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gerenciamento de Segurança da Informação (SGSI) dentro do contexto dos riscos da organização (ABNT NBR ISO/IEC 27001:2005).

- ISO 27002

A ABNT NBR ISO/IEC 27002:2005 é um padrão de diretrizes gerais de princípios para iniciar, programar, manter e melhorar a gestão da segurança da informação em um ambiente corporativo, ela é a renomeação da ISO 17799 e é um código de boas práticas de segurança da informação. Este padrão foi publicado pelo o governo do Reino Unido, que se tornou um padrão no ano de 1995 quando foi republicada pela British Standards Institution (BSI) como BS7799 (THE ISO 27000 DIRECTORY, 2011).

A norma ABNT NBR ISO/IEC 27002:2005 auxilia a uma organização a elaborar uma política de segurança em um curto espaço de tempo baseada em controles de segurança eficientes (INFORMABR, 2011).

- ISO 27003

A ISO 27003 tem como finalidade auxiliar a implementação de um SGSI com foco em segurança da informação. A nomenclatura dela é "A tecnologia da informação – Técnicas de segurança da informação de gestão da orientação de implementação de sistema." Esta norma em si é voltada, basicamente, para a segurança de sistema com finalidade de melhorar o SGSI (THE ISO 27000 DIRECTORY, 2011).

- ISO 27004

A ISO 27004 foi publicada no final de 2009 e fornece orientações sobre o desenvolvimento, utilização de medidas e medidas para avaliação da eficácia de um sistema de gestão da informação. Segundo o próprio site, esta norma destina-se a ajudar uma organização a medir a eficácia do SGSI *(Sistema de Gerenciamento de Segurança da Informação)*. O título atual é "A tecnologia da informação – Técnicas de Segurança – Gestão da informação de segurança – Medida" (THE ISO 27000 DIRECTORY, 2011).

- ISO 27005

Este padrão da série 27000 cobre a gestão de riscos de segurança da informação. De acordo com o site THE ISO 27000 DIRECTORY a norma fornece diretrizes para informação de gestão de riscos de segurança (SGRI) em um ambiente corporativo (THE ISO 27000 DIRECTORY, 2011).

- ISO 27006

Este padrão oferece diretrizes para o credenciamento das corporações que oferecem certificação e registro em relação a um SGSI, onde foi supervisionado pelo comitê da ISO SC 27. Seu título oficial é "A tecnologia da informação. – Técnicas de segurança requisitos para organismos de auditoria e certificação de sistemas de informação de gestão da segurança" (THE ISO 27000 DIRECTORY, 2011).

3.3 Detalhamento ISO 27002

A ISO 27002 trata da gestão da segurança da informação, esta norma é voltada para ambientes coorporativos onde a informação é o principal ativo do negócio por este motivo é temos a norma como base para elaboração do guia.

Tabela 1: Capítulos da ISO 27002

Capítulo	Descrição
1. Objetivo	Estabelecer princípios e diretrizes para iniciar, programar, manter e melhorar a segurança da informação em uma organização.
2. Termos e definições	São funções e procedimentos que devem ser medidos pela própria organização.
3. Política de Seguranças	Normas e procedimentos.
4. Segurança organizacional	Promove proteção dos recursos e serviços da organização.
5. Classificação e controle dos ativos de informação	Mantem a proteção adequada da organização.
6. Segurança ambiental e física	Define áreas de circulação restrita e a necessidade de proteção dos recursos e serviços.
7. Gerenciamento das operações e comunicações	Manter a operação segura e correta dos recursos da informação.
8. Desenvolvimento de sistemas e manutenção	Visa à melhoria e continuidade dos SI da organização.
9. Gestão de continuidade do negócio	Trata de um plano de ação.
10. Conformidade	Auditoria, controle e fiscalização.

Os tópicos apresentados na tabela estão regulamentados na ABNT NBR ISO/IEC 27002:2005 que normatiza a Política de Segurança da Informação, e foi criada sob padrões internacionais, como o *British Standart*. Afim de garantir a segurança da

informação, sugere-se 12 itens, cuja estrutura também foi adotada pela norma brasileira que converteu a 17799 em 27002 a partir de 2005. A Tabela 1 apresenta segundo Casanas e Machado (2001), os capítulos da ISO 27002 sobre a Segurança da Informação.

3.4 Políticas de Segurança da Informação

A política de segurança tem um papel importante em todas as organizações. Seu desenvolvimento é o primeiro e principal processo de segurança no meio corporativo. É por meio dessa política que se definem todos os aspectos envolvidos na utilização dos recursos (NAKAMURA; GEUS, 2007).

A politica de segurança é um manual de normas e procedimentos elaborado a partir do modelo de negócio da empresa, sendo este baseado na ISO 27002.

A ISO 27002 atende diversos temas relacionados à segurança da informação, contendo mais de 100 controles que devem seguidos para garantir a qualidade dos recursos. Uma certificação é a forma mais clara de mostrar para a sociedade que a empresa está dentro dos padrões e fornece segurança de suas informações (CASANAS; MACHADO, 2001).

Segundo a tabela 1, que trata dos capítulos da ISO 27002, no item 3 a política de segurança passa a ser uma consequência da aplicação bem sucedida da norma, na medida em que se enquadra na ISO 27002 a empresa deve buscar formas de manter-se segura e pode utilizar como parte desse mecanismo a política de segurança.

Além de aspectos práticos de software e hardware, uma política de segurança também precisa estabelecer os níveis de usuário, direção e técnico, para que fiquem claras quais as responsabilidades cabíveis a cada um deles, e deve ser flexível para os casos de mudanças ou adaptações, pois os mecanismos de segurança variam com o passar do tempo. É necessário que todos os envolvidos (funcionários, alta direção e gestores de sistemas e redes) se comprometam com as regras acordadas na elaboração da política de segurança (BAUER, 2006).

De acordo com Mitnick e Simon (2003) no livro "A arte de enganar", o consultor de segurança Bruce Scneier afirma que "a segurança não é um produto, ela é um processo", e não é um problema para a tecnologia e sim para as pessoas.

Toda empresa tem necessidade de elaborar a sua própria política de segurança de informação, pois uma solução segura para determinada empresa, pode não ser uma solução recomendada para outra, por terem negócios diferentes. Além disso, a segurança não é trivial: precisa ser tratada por profissionais qualificados em uma organização, caso contrário, a mesma pode estar vulnerável a ataques, como afirma Nakamura e Geus (2007, p.188):

> A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações. A necessidade de estabelecer uma política de segurança é um fato realçado unanimemente em recomendações provenientes tanto do meio militar [...] como do meio técnico [...] e, mais recentemente, do meio empresarial [...].

Uma política de segurança deve ser imprescindível para as empresas que lidam com informações em meio eletrônico. Embora ela não deixe a rede totalmente segura e a prova de *hackers*, ela mantém seu sistema mais confiável, capaz de anular as tentativas casuais de invasão e se, e somente se, uma tenha sucesso, o plano de

contingência será capaz de sanar quaisquer danos causados pelos invasores (NAKAMURA; GEUS, 2007).

A ISO 27002 prepara qualquer corporação para criar sua política de segurança, seja qual for o negócio da mesma. Contudo não se pode deixar de citar que estas regras são moldadas para uma organização em si e isto não implica que as mesmas regras sejam seguras em outra, por serem ambientes e/ou negócios diferentes.

3.4.1 Diretrizes

O planejamento de uma política de segurança deve ter como diretriz, procedimentos que incluam regras que englobem todos os pontos e que sejam obedecidas por todos da organização. Tais regras devem explicar o funcionamento e uso dos recursos e os controles para proteger a informação (NAKAMURA; GEUS, 2007).

3.4.2 Pré-Requisito

Nakamura e Geus (2007) entendem que o planejamento de uma política de segurança exige uma visão abrangente, de modo que os riscos sejam entendidos para que possam ser enfrentados. O apoio da gestão é extremamente importante, o que faz com que os recursos financeiros para as soluções sejam atendidos.

3.4.3 Objetivos

Para a ABNT NBR ISO/IEC 27002:2005, é necessário estabelecer diretrizes para gerenciar a gestão da informação em um ambiente coorporativo. Com os objetivos definidos, o controle tem como finalidade atender os requisitos identificados na elaboração do projeto. A norma pode ser utilizada como um guia prático para criação de boas práticas de Segurança da Informação e dos recursos em uma organização.

3.4.4 Implantação

O significado de implantar significa iniciar, realizar, executar. Para Nakamura e Geus (2007) esta pode ser a parte mais difícil da política de segurança, sua criação e definição envolvem conhecimentos diversos que não estão ligados diretamente à tecnologia e sim com aspecto organizacional e comportamental dos envolvidos.

Com a divulgação contínua, este documento deve fazer parte cultural da organização algumas formas de divulgação são:

1. Comunicação interna (e-mails e intranet);
2. Reuniões;
3. Treinamentos contínuos e específicos sobre os recursos de TI.

3.4.4 Consequências

Manter o ambiente da organização seguro e estável até a elaboração da política de segurança e certificação da ISO 27006.

4. Proposta

Este trabalho antecede a criação da política de segurança para a empresa em estudo. É embasado na experiência, estudo de caso e pesquisa científica a fim de propor uma solução para elementos que compõe as boas práticas de segurança.

A empresa em estudo não será revelada, por motivos de segurança. Nesse trabalho identificam-se pontos vulneráveis que podem ser utilizados e assim ocasionar sérios problemas para a organização. É como apresenta Nakamura e Geus (2007): alguém que se venha do "lado negro da força" contra a organização. Com base na ISO 27002, elabora-se este guia, para que, em um primeiro momento, a organização corrija as falhas detectadas e em seguida crie sua política de segurança.

A ISO 27002 é a principal referência sobre Segurança da Informação, pois aborda todos os aspectos relacionados em uma organização. Alguns autores foram estudados para chegar a esta pré-criação da norma, mas o livro que considera-se como a segunda literatura mais importante da área de Segurança da Informação é o livro Segurança de Redes em Ambientes Coorporativos (NAKAMURA; GEUS, 2007), voltado diretamente para este assunto e aborda todos os temas e obstáculos encontrados normalmente nas empresas.

Com esse trabalho em mãos, a empresa poderá definir suas futuras regras e entender seus problemas para que diminua os riscos e assim formaliza seu modo de trabalho em relação à segurança da informação, criando sua Política de Segurança, conforme ilustra a Figura 1:

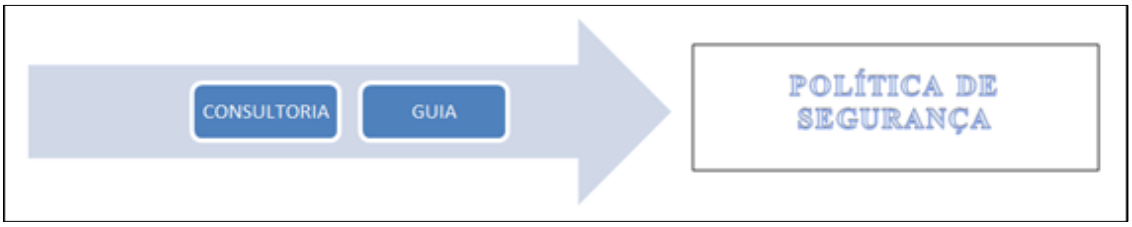

Figura 1: Gráfico informativo de como o trabalho pode ser utilizado pela organização em estudo.

Para tanto esse trabalho está dividido nas seguintes etapas como mostra a Tabela 2:

TABELA 2: Etapas realizadas durante este trabalho

Etapa	Descrição
CONSULTORIA	Diagnóstico da situação atual da empresa em estudo; Pesquisa de caráter cientifica sobre o assunto;
PROPOSTA/GUIA	Ponto que será entregue a organização, sugestões corretivas e de manutenção.
POLÍTICA DE SEGURANÇA	O Trabalho de Conclusão de Curso (TCC) e o GUIA propiciarão à organização elaborar sua política de segurança com base em uma infraestrutura de TI sólida e segura.

1º - Levantamento de Informação sobre a organização:

Nesta etapa é realizada uma consultoria envolvendo a utilização dos recursos administrativos, técnicos e físicos. Com base nestas informações a organização terá em mãos sua situação real dos recursos da Informação e como eles estão sendo utilizados.

2º - Diagnóstico – Identificação de Riscos/Problemas:

Identifica os riscos e os problemas para a organização e os separa. Neste ponto foi exposto e classificado o que seria risco ou problema.

3º - Proposta

Embasado na ISO 27002 a proposta irá adequar a empresa corrigindo a problemática chegando a uma solução certificada.

4º - Construção do Guia:

Com base no passo anterior, tem-se a construção de um guia de boas práticas, corrigindo os problemas detectados e sugerindo ações para mitigar os riscos.

5º - Treinamento e divulgação de boas práticas:

Nesta fase, colocar-se-á na intranet da organização o Guia informativo buscando nortear as ações do departamento de TI, evitando problemas na má gestão dos recursos.

5. Desenvolvimento

5.1.1. Desenvolvimentos das práticas da empresa

5.1.2. Administrativas

- Comunicação

A empresa em estudo utiliza o serviço de e-mail gerenciado pelo BRMA e o Mozilla Thunderbird como cliente de e-mail padrão. A comunicação dentro da organização é realizada através de e-mail, e dos comunicadores MSN e SPARK. No caso do MSN não há gerenciamento da comunicação, sendo liberado de acordo com a necessidade. Não há ferramenta como o Proxy MSN para gerenciar o tráfego de mensagens deste aplicativo. Já o SPARK é monitorado e o tráfego é restrito a intranet gerando controle de mensagens.

- Sistemas Integrados de Gestão Empresarial (*SIGE*), ou Enterprise Resource Planning (*ERP*)

A organização utiliza o ERP LOGIX 10 da TOTVS e seu banco de dados é o INFORMIX da IBM. As aplicações citadas executam em servidores distintos que utilizam Sistema Operacional (SO) Linux. O backup do LOGIX é feito de forma manual e em fitas *dat*. O sistema utilizado pelos vendedores foi desenvolvido pela equipe de TI da própria empresa e é executado na plataforma PALM OS. Realizando-se

a importação e exportação em lote de pedidos através de outro sistema que é executado dentro da plataforma WINDOWS da Microsoft, que também foi desenvolvido internamente, fazendo a gravação destes pedidos na mesma base de dados do ERP LOGIX. A empresa não possui outras filiais, apenas a matriz localizada em Juazeiro do Norte - CE. O quadro atual dispensa o uso de tecnologias de rede à longa distância para fazer o acesso ao banco de dados utilizado pelo ERP diretamente.

5.1.2. Técnicas

A organização utiliza o SAMBA para compartilhar serviços entre sistemas heterogêneos e restringir a informação a pessoas não autorizadas. Com um sistema de login de domínio, cada usuário é único dentro da organização em estudo. Não existe um sistema de registro para verificar informação, o controle é apenas de direito de acesso. Para a troca de arquivos é destinada uma pasta pública onde todo o usuário tem livre acesso para trocar arquivos e o dispositivo USB é livre em todos os terminais.

A organização utiliza o antivírus F-SECURE para gerenciar todo o domínio de possíveis infecções e softwares maliciosos.

O Sistema Operacional padrão nos terminais é da Microsoft, sendo que nem todos estão na mesma versão. A tabela 3 apresenta distribuição das quantidades:

Tabela 3: Distribuição do Sistema Operacional da Microsoft na organização em estudo.

Sistema Operacional	Número de Terminais
Windows XP SP3	50
Windows Vista	3
Windows Seven	10

FONTE: Empresa em estudo

5.1.3. Físicas

- Centro de Processamento de Dados

Não há restrição de acesso à sala central de TI da empresa em estudo a pessoa alguma. Nesta sala encontram-se 4 servidores DELL e 4 PCs que fornecem serviços dentro da organização. O cabeamento não se encontra em estrutura adequada para a manipulação, conservação e organização. O switch está ligado com os cabos entrelaçados e não identificados sem condição alguma de ser gerenciado.

A organização dos servidores é mostrada na Figura 2.

Figura 2: Organização dos servidores. As setas indicam o cabeamento.

No total, são *4 Switches* e *3 Hubs* conforme pode ser observado na figura 2. O desempenho da rede nas áreas conectadas aos *Hubs* é inferior porque este equipamento trabalha em *Broadcast* que implica em envios de pacotes sem gerenciamento.

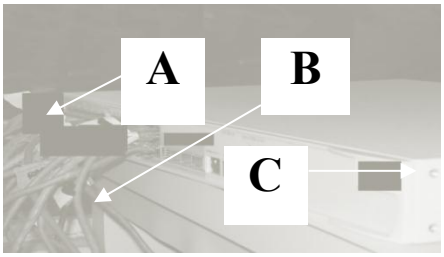

Figura 3: Switch da marca 3COM sobre a mesa com alguns cabos identificados de forma artesanal. A – Papel com a nomenclatura; B – Cabos; C - Switch

Quanto ao uso de cabo, o utilizado na empresa em estudo é o CAT5e. Sua proteção e/ou revestimento só existe nos pontos que ficam expostos ao sol. A rede sem fio não tem qualidade desejável, a não ser para o acesso a Internet e mesmo assim o usuário necessita do discador do BRMA instalado em sua máquina. Isso gera trabalho desnecessário para o suporte.

- Circuito Fechado de Televisão (*CFTV*)

A organização conta com 8 estações equipadas com placa de vídeo da *Geo Vision* com 16 canais e cada um com o Sistema Operacional Microsoft Windows XP SP3. Alguns desses terminais não ficam em sala isolada e não tem a proteção correta. As câmeras de monitoramento são conectadas às estações conforme indica o exemplo na figura 4.

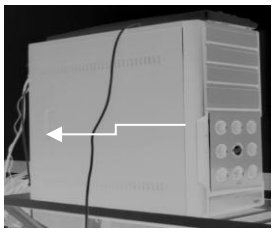

Figura 4: Uma das estações de CFTV da empresa a seta indica os cabos das câmeras.

Cada estação é responsável por guardar 30 dias de monitoramento auto-gerenciado, ou seja, ao completar o período o dia mais novo substitui o dia mais antigo armazenado.

Este serviço é restrito apenas a INTRANET e somente o Departamento de Tecnologia tem acesso a essas imagens.

Figura 5: Software monitorando o ambiente.

- Rede sem fio (*Wireless*)

A organização conta com 5 pontos de acesso a rede sem fio mas ela utiliza este meio de transmissão de dados de forma secundária, por não apresentar um número de equipamentos favorável que utilize esta tecnologia, sendo que apenas 8% dos usuários utilizam este recurso.

A principal utilidade é facilitar o trabalho de pessoas terceirizadas que necessitam de algum serviço tecnológico da organização. Para isso é necessário que tenham um IP configurado no Departamento de TI, senha da rede e o discador do BRMA instalado para então acessar a Internet.

O *Service Set Identifier (SSID)* é exposto para que seja visível para estes usuários e o raio é baixo, ficando restrito apenas a área da empresa. Mesmo que esta senha chegue a ser distribuída para pessoas externas, não seria possível acessar a rede de um ponto distante.

5.2. Diagnóstico

O diagnóstico trata em dispor a organização uma classificação dos fatores problemáticos que podem causar um forte impacto. Abaixo, a tabela 4 informa e classifica e resume os principais pontos do diagnóstico.

Tabela 4: Classificação dos principais pontos do diagnóstico em fator de risco ou fator problema

Fator	Risco	Problema
Não ter um Link de Internet para Backup.	X	
Software não licenciado.		X
Servidor de Internet proprietário.		X
Rede cabeada/sem fio não monitorada.	X	
Não ter comunicador interno.		X
Câmeras de vigilância não monitoradas e sem a proteção correta.	X	

Considera-se que o risco é um problema que ainda não ocorreu, e seu impacto deve ser estabelecido pela organização. Já o problema pode ser entendido como o pós-risco – o risco de acontecer algo se concretiza e gera o problema.

5.2.1. Administrativas

- Comunicação

A organização enfrenta problemas com a comunicação, não por fator tecnológico e sim por falta de cultura dos membros da instituição, que não têm o hábito de passar e-mails para fins de registro e documentação. Sendo assim, quando um usuário deixa a organização, não há como recuperar as informações com as quais ele trabalha. A comunicação é sempre de caráter pessoal gerando diversos problemas no meio organizacional.

O gerenciamento e armazenamento da comunicação gera uma documentação que dará suporte a futuros problemas e ajudará a encontrar uma solução.

- ERP

Ao se tratar de Segurança da Informação o ERP atende às necessidades da organização, liberando o acesso customizado ao usuário, ou seja, cada módulo do sistema é liberado de acordo com a função do funcionário. O problema neste ponto é a interpretação da Informação, pois o ERP gera diversos relatórios com dados que para o usuário comum não chega a ser Informação. O problema neste ponto é se a informação chegará às pessoas não autorizadas de forma impressa.

O Backup deste sistema é realizado de forma externa ao aplicativo e manual. O *Administrador de Banco de Dados* necessita estar fisicamente na organização para trocar a fita e realizar a cópia de segurança.

5.2.2. Técnicas

- BRMA

O BRMA é uma ferramenta de gerenciamento que funciona no SO Linux, que promete gerenciar e manter a rede segura. No entanto, em determinados momentos, sua inflexibilidade gera problemas. A Tabela 5 exemplifica esses pontos.

Tabela 5: Riscos do BRMA

Risco	Por quê?
Interface gráfica não compatível com linha de comando	Nem todos os recursos que são possíveis fazer por linha de comando é possível na interface gráfica.
Executa rotinas sem consultar o administrador	Após reiniciar algumas vezes o BRMA faz uma verificação no disco sem consultar o administrador, deixando por horas a internet indisponível.
Falha no gerenciamento de e-mails	Existe uma falha que, por algum motivo, a conta de qualquer um usuário pode ser desabilitada e os e-mails são perdidos para os que usam a WEB.

O BRMA não tem flexibilidade no gerenciamento de tráfego de informação, por esse motivo não é possível ter acesso ao conteúdo dos pacotes. Não existe um gerenciamento de MSN interno com o gerenciamento de Internet, para fazer isso é necessário adquirir outra ferramenta da BRCONECTION, montar outro servidor à parte e conectar no BRMA para ter o controle.

O uso de discadores e/ou aplicativos para acessar a internet traz uma perda de desempenho simplesmente porque para alguém acessar a internet, precisa passar pelo departamento de TI para que algum técnico faça essa instalação e configure corretamente.

- Gerenciamento do comunicador

O fato do comunicador não ser gerenciado e sim liberado de acordo com a necessidade gera uma falha de segurança na qual não é possível identificar as atividades suspeitas que prejudiquem o bom funcionamento da rede. Como por exemplo, algum usuário

recebe algum arquivo infectado, nesse caso provavelmente só seria possível descobrir quem recebeu mas não quem enviou.

- Windows XP

Com a descontinuação do Sistema Operacional Microsoft Windows XP, não será mais possível receber atualizações diretamente no Kernel, e o suporte ao mesmo não existirá mais e com o passar do tempo se tornará obsoleto e vulnerável a ataques.

5.2.3. Físicas

- Centro de Processamento de Dados

O acesso à sala não é restrito, pois qualquer pessoa interna ou externa a organização tem acesso a este ambiente.

Todos os serviços tecnológicos da organização se encontram nesta sala, tornando-os vulneráveis. Nada impede que um elemento entre na empresa em horário não comercial e execute algum ato malicioso como o roubo de algum recurso que afete a TI e a organização.

- Cabeamento Estruturado

O cabeamento estruturado da organização encontra-se em pontos cruciais expostos à sujeira e poeira. Alguns pontos passaram, em média, entre 5 e 10 anos sem a manutenção e a proteção correta, correndo-se o risco de rompimento proposital ou acidental, parando totalmente o uso da rede.

- Circuito Fechado de Televisão (*CFTV*)

As câmeras de vigilância estão instaladas em pontos estratégicos para monitorar a movimentação dentro da organização. O problema neste ponto é o armazenamento das informações, que se encontra em computadores que ficam expostos em pontos vulneráveis, correndo o risco de, em um evento malicioso, o malfeitor danificar estas informações e/ou até mesmo remover o gabinete, pois não existe uma proteção adequada.

Todo esse sistema de monitoramento encontra-se dentro da mesma rede de dados convencional, e o monitoramento é feito de forma remota, mas não interna ao sistema. É utilizado o protocolo de Virtual Network Computing (VNC) fazendo o acesso direto ao Sistema Operacional, tornando o mesmo obsoleto, por trazer além das imagens que são atualizadas do monitoramento tem o tráfego das imagens do Sistema Operacional.

- Rede sem fio (*Wireless*)

Apenas uma senha impede o acesso à rede, seu SSID se encontra exposto. Mesmo o raio sendo restrito e/ou baixo, ficando apenas dentro da organização, nada impede que um funcionário que tenha acesso à senha use um equipamento e faça movimentações indevidas. Não existe um sistema que registre as ações da rede e identifique quem, quando e o que foi acessado.

Ao acessar este serviço o usuário se conecta diretamente a rede de dados da organização, tornando um risco ainda maior, pois trafegam informações de caráter confidencial.

5.3. Propostas de segurança

5.3.1. Administrativas

Segundo o item 9 da ISO 27002, que trata de *Segurança física e do ambiente* relacionado à prevenção, o acesso físico não autorizado à hardware e software da organização, e as instalações físicas devem se manter em locais seguros e não visíveis, com barreiras e controle de acesso. Com base neste capítulo são propostos os seguintes itens:

- Centro de Processamento de Dados

O item 9.1.2 *Controle de entrada física* sugere que as áreas sensíveis que tenham um forte impacto sejam protegidas por controles aprimorados de entrada para assegurar que somente pessoas autorizadas tenham acesso. Dessa forma fechaduras com biometria e/ou cartões, outros dispositivos mais simples e sensores de presença para controlar o acesso.

- Cabeamento Estruturado

O item 9.2.3 *Segurança do cabeamento* descreve que o cabeamento de rede seja protegido visualmente e passado por conduítes. Deverá ser feita uma correção no cabeamento estruturado da organização de modo que seja corrigido e ocultado os pontos onde são vulneráveis e são vistos facilmente.

- Circuito Fechado de Televisão (*CFTV*)

O item 9.2.1 *Instalação e proteção do equipamento* afirma que os equipamentos devem ser protegidos para reduzir os riscos de ameaças e qualquer evento que comprometa o registro das informações bem como o acesso não autorizado. Sugere que tais computadores sejam isolados e colocados em locais discretos onde não fique visível.

- Rede sem fio (*Wireless*)

Segundo o item 10.6.1, *Controle de redes*, é necessário que sejam controladas de forma a proteger de ameaças e manter seguro serviços que utilizam este meio. Para isso, convém que o raio de acesso seja restrito apenas ao território da empresa e o SSID seja oculto para dificultar o acesso de pessoas de fora da organização.

5.3.2. Monitoramento da comunicação

De acordo com o item 10, *monitoramento*, da ISO 27002, que tem como o objetivo detectar atividades não autorizadas de processo de informação que convém que os sistemas sejam monitorados e os eventos de segurança sejam registrados e o item 10.10.2 informa que as atividades do usuário, exceções e outros eventos de segurança da

informação sejam produzidos e mantidos por um determinado período de tempo a fim de facilitar futuras investigações e monitoramento de controle de acesso.

5.4. Guia de boas práticas

5.4.1. Rotinas de manutenção e controle

Este guia propõe algumas mudanças nas rotinas do setor de TI da organização como algumas ferramentas de gerenciamento. Tais rotinas necessitam ser efetuadas de acordo com a Tabela 6.

Tabela 6: Rotinas do departamento de TI

Frequência	Ação	Benefícios
Diária	• Verificar log do gerenciador de internet. • Analisar fluxo da rede. • Backup do banco de dados do ERP. • Verificar disponibilidade do CFTV.	Manter os serviços ativos e a confiabilidade, integridade e disponibilidade da informação.
Semanal	• Mudar senha do root. • Fazer backup das imagens geradas no CFTV. • Executar backup das pastas compartilhadas pelos setores.	
Mensal	• Simular falta de energia. • Verificar cabeamento.	Garantir a disponibilidade dos serviços da organização.

Com estas rotinas aplicadas e mantidas, espera-se obter um alto ganho na qualidade do serviço relacionado à segurança da informação, pois todas as áreas estarão constantemente monitoradas e seu impacto será menor.

5.4.2. Administrativas

- Comunicação

Para monitorar o tráfego de mensagens do protocolo MSN de forma transparente, sugere-se a utilização do MSN-Proxy, que pode ser instalada na mesma máquina que executa o Squid, sem a necessidade de outro terminal executando a aplicação, como ocorre no BRMA.

MSN-Proxy: É uma ferramenta de gerenciamento de mensagens que monitora todo o tráfego do MSN em uma rede, seu banco de dados é o mySQL e sem a necessidade de instalação nos SO dos clientes, é possível armazenar, controlar os contatos e ver troca de arquivos de todos os usuários da rede. Este serviço não necessita de um servidor exclusivo para ser executado, como o software Messager Policy da BRMA, e ao contrário deste, o MSN-Proxy é gratuito.

- ERP

Trocar a senha do administrador (denominado de admlog) a cada 15 dias e verificar diariamente os acessos deste usuário.

5.4.3. Técnicas

- BRMA

A falta de flexibilidade no BRMA implica em retrabalho para o pessoal de TI, com base nessa informação sugere-se a utilização do Squid que é um serviço utilizado no Linux que tem a mesma função de gerenciar aos acessos de internet, conforme a descrição abaixo.

Squid: Utilizar com o pacote autenticador chamado ncsa_auth o qual utiliza arquivos de senhas no formato htpasswd do apache para identificar os usuários fazendo o mesmo efeito do BRMA sem custo algum para a organização. Com esta ferramenta qualquer equipamento poderá fazer acesso a internet sem necessidade de configuração manual.

- Gerenciamento do comunicador

Gerar documentação de e-mails de forma contínua, com a finalidade de documentar todos os processos da organização. É recomendado utilizar o Elgg, que é uma ferramenta de rede social onde a organização terá o total controle da comunicação entre os usuários.

- Windows XP

Substituir o Windows XP por outro Sistema Operacional, da Microsoft ou de outra organização, como o Ubuntu, nos setores que utilizam apenas o ERP como aplicação.

5.4.4. Físicas

- Centro de processamento de dados

Restringir o acesso à sala dos servidores ficando restrito apenas à direção e membros do departamento de TI e utilizar fechadura com leitor de cartão a fim de registrar todas as entradas e documentar as tarefas realizadas.

- Cabeamento estruturado

O cabeamento deverá ser substituído por cat6e e isolado com as pontas blindadas e a sua passagem feita através de conduites de forma separada da rede.

- Circuito Fechado de Televisão (*CFTV*)

Os servidores de CFTV deverão ser removidos dos locais expostos e o tráfego deverá ser realizado em uma rede isolada com controle de acesso e deverá ser feito a centralização destes servidores para melhorar o desempenho quando houver a necessidade de um acesso remoto.

- Rede sem fio (*Wireless*)

Para garantir a segurança da rede sem fio, é proposto o ocultamento do SSID e troca semanal da senha de acesso nos pontos mais externos da organização, onde o contato

com o ambiente externo é mais próximo. Nas áreas mais internas não será necessário tal preocupação, pois o sinal não sai de dentro da organização por estar em uma sala no subsolo.

5.4.5. Contribuições das propostas da ISO 27002

As contribuições geradas partir do estudo da norma ISO 27002 para a organização oferece visões sobre as áreas que são afetadas diretamente e proporciona maiores condições de manter o ambiente seguro e estável até a elaboração de sua política de segurança. É claro que as correções sugeridas na proposta e no guia de boas práticas não excluem a necessidade de formalização da política de segurança, mas servem com ferramental para orientar as ações de modo manter o ambiente seguro até a finalização da mesma.

6. Considerações Finais

Com o aumento da tecnologia nas organizações, a informação passou a ser o seu maior ativo. Desse modo precisa ser tratada e protegida, pois é um dos fatores críticos de sucesso de qualquer corporação. Nesse contexto, algumas organizações não estão preparadas para utilizá-las e protegê-las causando uma problemática para a segurança e uma possível perda incalculável para a empresa, visto a grande relação das informações e o negócio da organização.

A proposta deste trabalho engloba uma análise de práticas administrativas, técnicas e físicas que são alvo da consultoria aqui executada, a fim de enquadrar o ambiente em normas reconhecidas de segurança, como a ISO 27002, apresentando como resultado uma proposta de correções e um Guia de Boas Práticas que visa a mantê-las e auxiliar a construção, posterior, da política de segurança. Para tanto, essa consultoria identificou e classificou os riscos e problemas da organização em estudo, sugerindo uma proposta enquadrada nos principais itens da norma utilizada como base.

Espera-se que com o Guia de Boas Práticas o departamento de TI seja capaz de manter as sugestões apresentadas e dessa forma proporcionar à empresa gerar sua política de segurança sob uma infraestrutura de TI segura e equilibrada, que é de fundamental importância para manter a integridade, disponibilidade e a confidencialidade das informações. Além disso, a política de segurança pode auxiliar na construção do padrão de comportamento que a empresa espera dos seus colaboradores quanto ao uso dos equipamentos e recursos disponíveis para acesso e tráfego das informações, pautados na ética e no cooperativismo. Através da elaboração da política, a corporação, como um todo, passará a visualizar a relevância do uso adequado dos recursos, gerando uma economia de custos com a manutenção destes e a qualidade na operacionalidade dos seus equipamentos.

Na elaboração do guia, observa-se que as normas, procedimentos e a futura política em si são fatores fundamentais em qualquer meio organizacional, o que vai diferenciar é o tipo de negócio da empresa. Após este trabalho a organização estará apta a elaborar sua política de segurança aderente à ISO 27002.

Aplicadas das correções sugeridas na proposta e da aplicação do guia elaborado por essa consultoria a organização por si só estará apta a iniciar a elaboração de sua política de segurança como extensão desse trabalho. Com a política elaborada, a empresa poderá iniciar o processo de certificação na ISO 27006 demonstrando aos seus clientes e colaboradores que suas informações estarão seguras e bem protegidas.

7. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS E TÉCNICAS – ABNT. *NBR ISO/IEC 17799:2005 – Tecnologia da informação* – Técnicas de segurança – Código de prática para a gestão da segurança da Informação. Rio de Janeiro: ABNT, 2005.

_____. *NBR ISO/IEC 27001:2005 – Tecnologia da informação* – Técnicas de segurança – *Sistemas de gerência da segurança da informação*. Rio de Janeiro: ABNT, 2005.

_____. *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.

_____. *NBR ISO/IEC 13335-1:2004 – Tecnologia da informação* – Técnicas de segurança – Tecnologia da informação - Técnicas de segurança - Gestão de informação e segurança de tecnologia de comunicações. Rio de Janeiro: ABNT, 2004.

BAUER, C. A. **Política de segurança da informação para redes corporativas**. Trabalho de conclusão do curso de Ciência da Computação. Novo Hamburgo: Centro Universitário Feevale, 2006. Disponível em: <http://tconline.feevale.br/tc/files/621.pdf>. Acesso em: 10 fev. 2011.

CASANAS, A. D. G; MACHADO, C. S. Impacto da Implementação da Norma NBR ISO/IEC 17799 – Código de Prática para a Gestão da Segurança da Informação – nas Empresas. **IXXI Encontro Nacional de Engenharia de Produção**, Salvador, 2001. Disponível em: <http://www.fatec.br/html/fatecam/images/stories/dspti_ii/asti_ii_material_apoio_3_seguranca_informacao_texto_base1.pdf>. Acesso em: 10 fev. 2011.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet – Parte I: Conceitos de Segurança**. Versão 3.1, Outubro de 2006. Disponível em: <http://www.cert.br >. Acesso em: 11 fev. 2011.

INFORMABR. Disponível em <http://www.informabr.com.br/nbr.htm#13>. Acesso em: 21 set. 2011.

MITNICK, K; SIMON, W. **Arte de Enganar**. São Paulo: Makron Books, 2003;

NAKAMURA, E; GEUS, P. **Segurança de redes em ambientes corporativos**. São Paulo: Novatec, 2007;

SERPRO – SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **Infra-Estrutura de Chaves Públicas Certificação Digital**. Disponível em:< http://www1.serpro.gov.br/publicacoes/tematec/pubtem46.htm>. Acesso em: 11 fev. 2011.

SOUZA, B. A. **Teoria dos Números e o RSA.** Dissertação de Mestrado, Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas (UNICAMP), 2004.

THE ISO 27000 DIRECTORY. Disponível em <http://www.27000.org>. Acesso em: 21 set. 2011.