POLÍTICA INTERNA DE SEGURANÇA DA INFORMAÇÃO DA SUCOSUL

Maikon Thiago Silva Santos[1]

RESUMO

Diante da grande competição e mobilização no mundo dos negócios, é indispensável à utilização de processos e práticas eficazes para a evolução dos serviços. As empresas, então, necessitam vencer um grande desafio, que é a padronização para o alcance da excelência. Por esses motivos, o objetivo do presente trabalho é a criação e a implantação da Política de Segurança da Informação (PSI) na SUCOSUL, demonstrando que o alinhamento entre a área de negócio e a tecnologia organizacional é um importante instrumento de gestão. Os esclarecimentos acerca do tema abordado serão realizados através de pesquisa de campo desenvolvida no ambiente organizacional a ser implantada a Política de Segurança da Informação e pesquisa bibliográfica do tipo exploratória, descritiva e explicativa, a qual se utilizará de livros impressos, artigos científicos e materiais disponibilizados na Internet, para discussão, interpretação e desenvolvimento do tema estabelecido. Dessa forma, serão mostradas as principais atividades do setor de TI da indústria desde sua criação até os procedimentos realizados no seu dia a dia para garantir a segurança dos recursos organizacionais. Também serão mostradas as dificuldades, exigências, ferramentas e procedimentos que são seguidos na hora de implantar uma PSI , a qual proporcionará facilidades estratégicas para o desenvolvimento dos negócios, tais como as vantagens competitivas, a diminuição de custos e padronização que possibilitarão um crescimento futuro da indústria.

Palavras-chave: Desenvolvimento da Indústria; Gerenciamento do Ambiente; Implantação; Infraestrutura de Rede; Segurança da Informação; Política de Segurança da Informação.

[1] Formado em Licenciatura Plena em Informática pela UNIT, atuando profissionalmente como professor dos Cursos Técnicos em Informática e Informática para Internet desde 2014.
e-mail: maikonthiagoss@gmail.com

1 INTRODUÇÃO

No contexto atual de desenvolvimento e avanço da tecnologia, a área de TI obteve um grande crescimento no mercado, alcançando lugar de destaque e desempenhando papel decisivo nas diversas organizações. Por esses motivos, o alinhamento estratégico da Política de Segurança da Informação surge com novas oportunidades para o negócio, gerando redução de custos, melhorando a eficiência e qualidade dos serviços, por meio da padronização e gerenciamento de cada processo.

O presente artigo abordará as normas e padrões de TI relacionados à implantação da PSI no ambiente da empresa SUCOSUL, localizada na grande Aracaju, e relatará os vários problemas decorrentes da sua infraestrutura de rede precária, tais como a instabilidade da rede corporativa e o comprometimento da segurança dos dados e informações tratadas na empresa. Dentre as causas desses problemas, será abordado a ausência de métodos de controle de acesso à internet dos usuários, a ausência de domínio para o gerenciamento desktops, DVRs (gravador digital de vídeo), notebooks e smartphones dos usuários e clientes, e a resistência dos funcionários a se adequarem às normas de segurança.

O artigo, então, tem por objetivo mostrar os pontos relevantes decorrentes da implantação da PSI com a utilização de normas e padrões da Tecnologia da Informação na indústria SUCOSUL, os quais podem possibilitar uma eficiente melhoria e estabilidade nos serviços e na segurança da informação, quando a empresa utilizá-las de forma consciente, sistemática e automatizada, dispondo de um fácil acesso para os componentes, dando-lhes, assim, possibilidades de evolução estruturada do seu negócio. Também serão contrapostos os pontos negativos advindos anteriormente e durante todo esse processo, projetando os ganhos e benefícios da sua correta estruturação.

Dessa forma, sendo a estratégia tão importante para as empresas e sendo o papel da área de TI tão significativo para o crescimento e desenvolvimento dos negócios e dos benefícios da competição de mercado, o presente trabalho visa ampliar os conhecimentos adquiridos no curso de Especialização em Gestão de Redes de Segurança da Informação na Faculdade de Administração e Negócio de

Sergipe, de maneira a estabelecer uma padronização adotada no gerenciamento do ambiente de acordo com a PSI.

No desenvolvimento desse artigo, o procedimento metodológico utilizado foi a pesquisa de campo desenvolvida no ambiente organizacional a ser implantado a infraestrutura de redes, e a pesquisa bibliográfica, que abordou e explicou o tema através de fontes secundárias, com referenciais teóricos publicados em materiais já elaborados. O material posto e utilizado na pesquisa foi obtido por meio de vivência, acompanhamento das mudanças na empresa e participação dos responsáveis da TI, além de livros impressos, artigos científicos e materiais disponibilizados na Internet, os quais embasaram, fundamentaram o trabalho e deram consistência aos dados expostos nesse artigo. Por meio dele foi possível discutir sobre o tema proposto, relatando e analisando o impacto da implantação da PSI no gerenciamento do ambiente organizacional.

A pesquisa foi do tipo exploratório, descritivo e explicativo. Exploratória porque se buscou informações preliminares sobre o assunto, delimitando o tema e definindo os objetivos da pesquisa. Descritiva pelo fato de observar, analisar, interpretar e coletar os dados dos fenômenos. Explicativa por buscar um conhecimento mais complexo e profundo, identificando as causas e razões que contribuem para a ocorrência dos fatos e explicando os fatores e os porquês dos mesmos.

Consonante com as informações expostas e observância dos impactos decorrentes da implantação da Política de Segurança da Informação e das medidas de segurança para melhor gerir o ambiente corporativo e industrial, será analisado todo processo de transformação na área de TI ocorrida na empresa em questão, observando os seus benefícios, malefícios e os objetivos na eficiência e melhor gestão dos serviços.

2 DESENVOLVIMENTO

2.1 POLÍTICA INTERNA

A Política Interna de Segurança da Informação é um documento formal de grande relevância, utilizado como orientação para utilização dos ativos da tecnologia,

encontrando-se fundado em diretrizes da Segurança Informação (SI). Por essa razão, é necessário compreender o que vem a ser a SI e qual a sua importância para o compartilhamento e a proteção de informações.

A partir da sua denominação, já é possível esboçar uma ideia do seu significado e da sua abrangência. Por tal, a SI tem por objetivo proteger, frente aos diversos tipos de ameaças, dados e informações de valor que encontram-se guardados para uso individual ou expostos para consulta ou aquisição de uma organização ou indivíduo.

Cabe salientar que a proteção promovida pela SI não está restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento, mas a todo sistema em geral, por meio da aplicação de três princípios, a citar, a confidencialidade, a integridade e a disponibilidade, a seguir expostos:

Integridade: somente as alterações autorizadas pela organização ou indivíduo devem ser realizadas nas informações;

Confidencialidade: somente as pessoas autorizadas pela organização ou indivíduo podem ter acesso a determinada informação;

Disponibilidade: a informação ou dado deve estar disponível para as pessoas autorizadas, quando estas necessitarem acessá-las.

2.1.1 OBJETIVO DA POLÍTICA INTERNA

O setor de Tecnologia da Informação (TI) da SUCOSUL com total apoio da diretoria tem por objetivo estabelecer e implementar a presente Política Interna de Segurança da Informação, a qual é estendida a todos os seus colaboradores, visando a proteção das informações dos diversos tipos de ameaças que podem interferir no bom andamento do negócio, além da minimização dos riscos, da integração dos dados como forma de otimizar e maximizar a qualidade e proteção das atividades desenvolvidas no ambiente de trabalho, bem como estruturar sua rede de informações.

2.1.2 APLICAÇÃO DAS RESPONSABILIDADES

Ferreira e Araújo (2003) propõe a aplicação de responsabilidades e regras nas diferentes áreas da entidade. Seguindo os seguintes elementos:

- ✓ comitê de segurança da informação;
- ✓ proprietário das informações;
- ✓ área de segurança da informação;
- ✓ usuário das informações;
- ✓ recursos humanos.

Abaixo, é apresentado cada elemento:

1) Comitê de segurança da informação

O Comitê tem por função divulgar e estabelecer os procedimentos de segurança, bem como analisar a política periodicamente, ou a qualquer momento que seja necessário. Também deve buscar o envolvimento de todas as áreas da organização: comercial, jurídica, negócio, financeira, auditoria entre outras, conforme a estrutura da empresa.

Sugere-se que o conteúdo das reuniões realizadas seja relatado em atas. Ainda: em um determinado intervalo de tempo, que pode ser semestral, deve-se elaborar um relatório de avaliação da efetividade do sistema de controles de segurança, incluindo as deficiências detectadas com as respectivas recomendações para análise da administração da empresa. (FERREIRA; ARAÚJO, 2003, p. 44)

2) Proprietário da informação

O proprietário da informação é o responsável pela autorização para acesso da mesma. Ferreira e Araújo (2003) aconselham que estes profissionais devem ser da gerência de negócio da organização, pois serão afetadas caso alguma informação torne-se corrompida, perdida ou pública.

É recomendado que se realize a identificação dos proprietários da informação dos dados críticos e em seguida dos demais profissionais, ainda no início da implantação da política da informação.

3) Área de segurança da informação

Esta área é responsável pela proteção dos ativos de segurança. Suas responsabilidades incluem:

- ✓ fazer cumprir a política de segurança da informação;
- ✓ definir, implementar e revisar os controles;
- ✓ identificar os riscos inerentes e residuais da segurança;
- ✓ definir os critérios e procedimentos para a realização da classificação da informação, protegendo o que for mais crítico;
- ✓ avaliar os procedimentos de segurança, analisar os seus resultados e discutir as melhorias necessárias em relação a eles;
- ✓ definir soluções de segurança antes da implementação e durante a manutenção; elaborar programas de treinamento para capacitação de usuários e proprietários da informação;
- ✓ desenvolver, implementar e manter planos de continuidade os quais visem garantir as operações em casos de desastre e indisponibilidade dos sistemas de informação;
- ✓ monitorar o uso da web e do tráfego de mensagens de correio eletrônico. (FERREIRA; ARAÚJO, 2003, p. 45).

4) Usuários das informações

Todos os indivíduos que acessam as informações da organização são usuários, seja funcionário, seja contratado da empresa. Cabe aos usuários:

- ✓ entender, respeitar e fazer cumprir a política de segurança;
- ✓ utilizar as informações apenas para os propósitos do negócio;

✓ informar imediatamente ao canal de comunicação disponível qualquer incidente ou violação de segurança. (FERREIRA; ARAÚJO, 2003, p. 46).

5) Recursos humanos (RH)

O departamento de Recursos Humanos é responsável em criar as devidas penalidades para aplicar quando ocorrer o desrespeito à política. Este setor deve relatar a saída ou afastamento de colaboradores para a repartição da Tecnologia da Informação, para que este realize as medidas cabíveis na administração de acesso aos sistemas da organização.

Além disso, o RH deve contribuir com a TI nos planos de treinamento e educação para a implementação e manutenção da política de segurança, bem como na coleta de assinaturas do Termo de Responsabilidade de Segurança da Informação.

2.1.3 ORIENTAÇÕES SOBRE ANÁLISE E GERÊNCIA DE RISCOS

Independente dos meios e formas de proteção implementados na empresa, esta encontra-se sujeita a ocorrência de incidentes que podem vir a ultrapassar as barreiras impostas pela Política Interna de Segurança da Informação. Nessas situações a orientação é que as atividades sejam parcialmente ou totalmente cessadas para anular ou reparar as adversidades surgidas dependendo da sua criticidade, acompanhando a sequência de passos para neutralização através da análise das circunstâncias que induziram o aparecimento do problema, para aplicação de subsequentes soluções e consequente melhoramento.

Portanto, deve-se direcionar a atenção a possíveis situações futuras, incertas e desconhecidas quando da sua ocorrência, como forma de conversão dos resultados negativos em pontos positivos, através do planejamento de identificar, analisar e combater as áreas de riscos, desenvolvendo, assim, as prioridades de ações, os investimentos necessários e os caminhos para o controle das vulnerabilidades.

2.1.4 CONSEQUÊNCIAS DE VIOLAÇÕES À POLÍTICA INTERNA

Caso os procedimentos e normas de Segurança da Informação estabelecidos na presente Política Interna sejam violados por motivos diversos como fraude e negligência, a empresa, representada pela Diretoria ou Presidência, possui o direito de buscar respaldo legal ou adotar punições administrativas aos usuários responsáveis, a depender da gravidade do ato praticado. Por esse motivo, é de extrema relevância a conscientização dos colaboradores quanto à aplicação da Política Interna, para que não aleguem desconhecimento das suas diretrizes como forma de isentar-se de culpa.

Sendo assim, as punições cabíveis aos respectivos casos irão desde advertências verbais e escritas, suspensões, desligamentos em casos de reincidência, segundo artigo 482 da CLT, e até uma eventual ação judicial. Em situações mais extremas que demandem processos criminais, o ordenamento jurídico brasileiro prevê normas que abordam o tema, a exemplo da Lei n° 12.737/2012, que determina a tipificação de delitos informáticos para obtenção de vantagens ilícitas.

2.1.5 IMPORTÂNCIA DE MAPEAR OS PROCESSOS DE NEGÓCIOS E REGISTRAR OS RISCOS ASSOCIADOS PARA DESENVOLVIMENTO DA PSI

Diante de um momento de grande e constante competitividade, é necessário que a organização supra essa realidade, através da busca de meios e soluções para melhor estruturar e integrar seus processos, criando maior flexibilidade e agilidade em suas operações, motivos estes que justificam a necessidade da sua otimização.

O Mapeamento de Processo surge ,então, como uma ferramenta para gerenciamento dos processos existentes na empresa, que visa identificar, executar, documentar, medir, monitorar, controlar e principalmente melhorar o andamento dos processos, objetivando alcançar resultados estipulados nos planos de negócio.

O mapeamento também auxilia a organização a observar de forma nítida os pontos fortes, pontos fracos (pontos esses que devem ser aprimorados tais como: complexidade na operação, redução de custos, falhas de integração, tarefas de baixo valor agregado, retrabalhos, conter burocracias desnecessárias), além de ser uma

excelente forma de favorecer a percepção sobre os processos, aumentando consideravelmente a performance do negócio.

Por conseguinte, ao focar a importância do mapeamento de processo para o desenvolvimento da PSI, a empresa deve mapear todos os processos críticos ao negócio e realizar uma análise e avaliação de riscos capaz de identificar as vulnerabilidades, ameaças, impactos e níveis de riscos aceitáveis, com os respectivos controles e tratativas, de acordo com as suas estratégias, devendo ser revisado sempre que mudanças de impacto ocorram no ambiente.

Essa ferramenta revela-se, por fim, como meio importante para o alcance de objetivos essenciais, a exemplo da eficiência, inovação, controle, agilidade, conformidade, integração com a TI, dentre outros, razões estas que justificam a sua adoção.

2.2 SUPERVISÃO E CONFORMIDADE DOS SISTEMAS COMPUTACIONAIS

Para uma efetiva manutenção, adesão e divulgação da Política Interna de Segurança da Informação, é imprescindível a conformidade dos sistemas computacionais com as mudanças organizacionais e do próprio cenário tecnológico, por meio de fiscalizações e análises constantes das ações, dos colaboradores, dos produtos etc, com o objetivo de reparar as adversidades decorrentes de inobservância de procedimentos e padrões estabelecidos.

Porém, as análises internas não se mostrem suficientes, o que demonstra a necessidade de auditorias externas de Tecnologia da Informação para garantir o exame dos processos, sistemas e responsabilidades, como meio de verificar a sua conformidade e adequação com as metas da empresa e demais regulamentações.

Cabe ressaltar, que nas avaliações periódicas alguns controles serão realizados, a citar os preventivos, que buscam evitar a ocorrência dos problemas e incidentes, os detectivos, que buscam encontrar os erros e os corretivos, que buscam corrigir os problemas e minimizar seus impactos.

2.2.1 POLÍTICAS DE CONTROLE DE ACESSO A RECURSOS E SISTEMAS COMPUTACIONAIS

São de responsabilidade do setor de TI a liberação e o controle de acesso, sendo estes novos com a mudança de cargo ou setor e desligados da empresa, pois será liberado o tipo de nível de acesso de acordo com a necessidade, função e setor que o funcionário precisa para obter determinada informação, garantindo que somente os usuários autorizados consigam acessá-las.

Nessas situações incluem-se a exigência de alterações constantes de senhas, evitando a repetição, as quais devem conter no mínimo oito caracteres com distinção de letras maiúsculas, minúsculas e caracteres especiais (@,$,#,etc.), e caso o usuário tenha acesso a diferentes sistemas, as senhas utilizadas devem ser exclusivas para cada um.

Torna-se assim, obrigatória a assinatura de termos para ser permitida aos usuários e gestores de negócios a obtenção de recursos supracitados da TI, comprometendo-se aos direitos discriminados para acesso. Caso ocorra algum descumprimento do acordo assumido pelo colaborar, este será devidamente punido.

2.3 PADRÕES MÍNIMOS DE QUALIDADE DOS SISTEMAS

Este quesito é de suma importância, por abordar quais sistemas serão utilizados para auxílio do melhor andamento e controle confiáveis e eficazes do negócio. Além de assegurar que as informações que são tratadas pela SUCOSUL, estejam resguardadas com sistema de segurança atualizado e de qualidade.

Após aprovação e diagnóstico da PSI, foi verificado que a solução em padronizar os sistemas é a forma mais adequada de manter a qualidade e isto só será possível com a adoção dos modelos conhecidos internacionalmente, que são o COBIT, usado para o diagnóstico dos processos de TI, e o ITIL, escolhido para contribuir com o andamento e qualidade dos processos e serviços de forma centralizada.

2.4 CLASSIFICAÇÃO DAS INFORMAÇÕES

O parâmetro utilizado para classificação das informações foi o Princípio da Segurança da Informação: confidencialidade. Na qual foram rotuladas em:

- ✓ Irrestrita: São informações que podem ser publicadas e acessadas por qualquer pessoa, sem causar risco ou dano à empresa, a exemplo: informações publicadas no site ou portfólio da empresa.

- ✓ Interna: Estas podem circular dentro da organização com os devidos cuidados para não serem expostas, pois são capazes de interferirem nos planos ou operações do negócio, a exemplo: informações minuciosas sobre planos de construção de uma nova polpa mais concentrada e com menor custo, caso acabe nas mãos dos concorrentes antes do lançamento.

- ✓ Confidencial: Se acessadas por pessoas não autorizadas, levará a frustração dos planos ou danificar a segurança de toda SUCOSUL, a exemplo: vazamento a dados dos clientes, podendo receber algum processo ou causar fragilidade na confiança dos mesmos, levando-os a procurar a concorrência.

- ✓ Secreta: Quando o sigilo destas informações é quebrado, acarreta danos desastrosos na integridade de toda segurança da instituição, a exemplo: o acesso as contas da empresa de forma não autorizada, resultando em graves prejuízos financeiros ou até mesmo falência.

2.5 FUNDAMENTOS LEGAIS QUANTO À TECNOLOGIA DA INFORMAÇÃO

Em observância das normas jurídicas brasileiras e das cláusulas contratuais, os dados, os documentos e as informações produzidas por meio dos sistemas de Tecnologia da Informação são de propriedade exclusiva da empresa, da mesma forma que os softwares desenvolvidos pelos seus funcionários, possuindo como finalidade a utilização interna.

Dessa maneira, os sistemas, as criações, os dados e as informações devem ser utilizados em acordo com a garantia de posse dos seus responsáveis, como as cláusulas de confidencialidade, presente no contrato, o direito de autoria, regulado

pela Lei n° 9.610/98, o direito de propriedade industrial, previsto na Lei de Patentes n° 9.279/96 e os direitos de criação e utilização de software, abrangidos pela Lei n° 9.609/98. Tais normas são meios legais que impedem que as propriedades da empresa sejam violadas ou manipuladas, e que somente sejam utilizadas mediante autorização expressa dos seus proprietários de direito.

2.6 PROCEDIMENTOS DE PREVENÇÃO E DETECÇÃO DE VÍRUS

Para uma melhor eficiência na detecção e prevenção de vírus, deverá ser utilizado um firewall por hardware gerenciável da Cisco, posto que as informações tratadas são extremamente sensíveis e necessitam de um tratamento adequado e gerenciado, através de controles de acesso. Também será empregada a utilização de VPNs (Redes Virtuais Privadas), antivírus do tipo endpoint, que possibilitarão um melhor desempenho, controle, prevenção e verificação de vírus, além dos bastion hosts que são gateways instalados entre a rede externa e interna, como forma segurança de ataques.

2.7 PLANO DE TREINAMENTO EM SEGURANÇA DE INFORMAÇÕES

Desde a contratação de um novo funcionário até a permanência daqueles mais antigos é preciso que a empresa esteja ciente da relevância de capacitação e qualificação constante destes profissionais para que eles desempenhem da melhor forma as suas atribuições, através do aprimoramento das suas habilidades e competências.

Essas capacitações e qualificações derivam do treinamento condizente com as necessidades diárias e específicas desse departamento, em que se faz possível integrá-lo ao ambiente corporativo e fomentá-lo de aptidão ao manuseio dos equipamentos e setores, nesse caso, da segurança da informação.

Por esse motivo, no plano de treinamento serão tratados os seguintes temas:

- ✓ A internet e o correio eletrônico
- ✓ Os softwares de conversação instantânea

- ✓ Compartilhamento de arquivos
- ✓ Sites de conteúdo inapropriado
- ✓ Diretrizes quanto ao uso da Internet
- ✓ Realização de downloads e uso de mídias externas ou removíveis
- ✓ Execução de jogos e rádios on-line
- ✓ Senhas de acesso
- ✓ Recomendações sobre o uso do correio eletrônico (E-mail)
- ✓ Instalações de software

2.7.1 INTERNET E O CORREIO ELETRÔNICO

Com o advento do uso da internet e sua grande necessidade de utilização nas diversas empresas, surgiram problemas diretamente ligados a esta ferramenta.

Condutas alheias aos preceitos de crescimento individual e intelectual, através do acesso a sites de conteúdo discordantes, refletem diretamente na segurança interna dos computadores da empresa, uma vez que os acessos a tais sites ou o uso de programas específicos tornam a estrutura vulnerável, passível de invasão por “hackers” (piratas da internet), vírus de computador e uma infinidade de outros perigos virtualmente existentes.

Por tais motivos, medidas conscientes dos próprios funcionários se fazem necessário, além da implantação de um mecanismo que monitora todo o tráfego da rede, informando os sites acessados por cada usuário, inclusive demonstrando o dia/mês/ano e horário, o que permite ter uma melhor visão do que era acessado, quando e por quem, identificando computadores infectados por vírus e os usuários que persistem em acessar sites de conteúdo proibido ou que utilizam softwares que comprometem a segurança da rede interna.

2.7.2 SOFTWARES DE CONVERSAÇÃO INSTANTÂNEA (Instant Messengers)

Softwares de conversação instantânea, ou IM-Instant Messengers, são programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

Os IM surgiram como a solução para muitas empresas/setores que não possuíam linha telefônica externa ou que pretendiam reduzir custos com ligação, pois as sessões de áudio substituíam o telefone convencional e o envio de arquivos superava a remessa via correio, seja pelo fato de serem instantâneos, onde em menos de um minuto o arquivo já estava no micro do destinatário, seja pelo custo, que é zero.

O grande problema de se utilizar este tipo de software é que, uma vez conectado, o computador fica altamente vulnerável. As portas de entrada/saída ficam abertas, sem qualquer restrição de leitura ou gravação. Desta forma, vírus que exploram esse tipo de vulnerabilidade não encontram empecilhos para se instalarem e iniciarem os processos danosos, não só para aquele micro, mas para todos os que a ele estiverem conectados ou que estiverem em rede.

Essa foi é uma das formas com que muitos vírus adentram na rede de empresas e permanecem por muito tempo se replicando. Cabe visualizar a necessidade do seu uso, pesando sempre os prós e contras.

Exemplos de Instant Messengers: MSN Messenger, Yahoo Messenger, Skype, Facebook Messenger.

2.7.3 COMPARTILHADORES DE ARQUIVOS

Software muito utilizado e frequentemente encontrado instalado nos equipamentos são os compartilhadores de arquivos. Este tipo de software promove um compartilhamento universal de arquivos de todos os formatos, permitindo ainda ao usuário executar o referido arquivo on-line ou baixá-lo em seu computador.

O uso deste tipo de software é altamente nocivo, principalmente pelo fato de que, ao instalá-lo no computador, o usuário dá amplas permissões de leitura e gravação. Ou seja, ao se conectar através do software, o usuário não está somente lendo arquivos de outros computadores, mas também permitindo que outros usuários efetuem uma verdadeira varredura em seu disco rígido. Esta vulnerabilidade também é explorada pelos vírus e/ou por “hackers” que vasculham por redes passíveis de invasão.

Exemplos de Compartilhadores de Arquivos: Full Throttle, Kazaa, Morpheus, Napster, Mp3X, Utorrent.

2.7.4 SITES DE CONTEÚDO INAPROPRIADO

Muitos usuários acessam alguma “home page” com conteúdo inapropriados. O acesso a esses tipos de sites gera uma série de situações de extremo constrangimento, além do trabalho de conscientização que deve ser realizado junto aos setores no sentido de coibir este tipo de prática, alguns ajustes no servidor se fazem necessário, de modo a não permitir o acesso a uma série de sites cujo conteúdo vai de encontro aos interesses desta empresa.

2.7.5 DIRETRIZES QUANTO AO USO DA INTERNET

A internet deve ser utilizada para fins de complemento às atividades do setor, como ferramenta para busca por informações que venham a contribuir para o desenvolvimento de seus trabalhos.

Jamais devem ser utilizados para a realização de trabalhos de terceiros ou de atividades paralelas. O uso para fins pessoais, como a consulta a movimento bancário ou acesso a e-mail pessoal, deve ser realizado fora do horário de expediente.

O uso da rede WI-FI, ficará condicionado às solicitações dos responsáveis de departamento.

2.7.6 REALIZAÇÃO DE DOWNLOADS E USO DE MÍDIAS EXTERNAS OU REMOVÍVEIS

A tarefa de downloads deve ser vista com muito cuidado e sua realização feita somente em casos de extrema necessidade, mediante prévia solicitação à Gestão de TI, pois downloads muito grandes podem congestionar o fluxo de tráfego e comprometer sistemas que funcionam on-line.

Quanto ao uso de mídias externas ou removíveis, devido ao risco de contaminação de vírus na rede pelo uso não gerenciado de pen-drive, cd, dvd ou hd externo, todas as portas de unidades removíveis em nossos terminais serão bloqueadas.

Caso haja necessidade de uso, o responsável do setor deverá solicitar previamente à Equipe de TI a liberação de uso da unidade, que deverá realizar varredura da mídia e somente após a certificação de que não existam riscos, liberá-la para uso.

2.7.7 EXECUÇÃO DE JOGOS E RÁDIOS ON-LINE

Uma vez que não existe qualquer pertinência com as finalidades propostas por esta empresa, é terminantemente proibida a execução de jogos, músicas ou rádios on-line, visto que esta prática toma grande parte da banda de navegação de internet, dificultando a execução de outros serviços que necessitam deste recurso.

2.7.8 SENHAS DE ACESSO

Somente poderão acessar a Internet ou Sistema, usuários que tenham sido credenciados com suas senhas de acesso.

Cada setor deverá solicitar à equipe de TI, novos usuários que deverão ser credenciados para tal serviço, justificando quanto à necessidade do referido funcionário utilizar-se deste recurso.

A senha de acesso tem caráter pessoal, e é intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo.

A prática de compartilhamento de senhas de acesso é terminantemente proibida e o titular que fornecer sua senha a outrem responderá pelas infrações por este cometidas, estando passível das penalidades aqui previstas.

Caso o usuário desconfie que sua senha não é mais segura, ou de seu domínio exclusivo, poderá solicitar à Gestão de Informática a alteração desta.

2.7.9 RECOMENDAÇÕES SOBRE O USO DO CORREIO ELETRÔNICO (E-MAIL)

Como forma de possibilitar uma melhor e adequada utilização e manipulação do correio eletrônico algumas medidas são necessárias:

- ✓ Não abrir anexos com as extensões: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela Gestão de Informática, se não tiver certeza absoluta de que solicitou esse e-mail;
- ✓ Desconfiar de todos os e-mails com assuntos estranhos e/ou em inglês.
- ✓ Não reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida etc.;
- ✓ Não utilizar o e-mail da empresa para assuntos pessoais;
- ✓ Evitar enviar anexos muito grandes;
- ✓ Adotar o hábito de ler sua caixa de e-mails diariamente, de modo a evitar que se acumulem os e-mails.
- ✓ Utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito.

2.7.10 INSTALAÇÃO DE SOFTWARES

Qualquer software que, por necessidade do serviço daquele setor, necessitar ser instalado, deverá ser comunicado com antecedência à Gestão de Informática.

Fica permanentemente proibida a instalação de quaisquer softwares não-freeware sem licença de uso.

A Gerência de Informática poderá valer-se da sua autonomia para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei nº 9.609/98 (Lei do Software).

2.8 AUTONOMIA DA GESTÃO DE INFORMÁTICA

A Gestão de Informática tem total autonomia para atuar sobre os equipamentos da empresa, no que concerne aos seguintes tópicos:

- ✓ Realização de auditoria (local ou remota);
- ✓ A definição de perfis de usuários cujos privilégios não permitam a realização de atividades tidas como nocivas ao sistema operacional ou à rede como um todo;
- ✓ A instalação de softwares de monitoramento;
- ✓ A desinstalação de quaisquer softwares considerados nocivos à integridade da rede;
- ✓ O credenciamento/descredenciamento de usuários.

2.9 MEMBROS DA EQUIPE DE SEGURANÇA

Os servidores qualificados na área de TI são diretamente responsáveis pela implantação da Política de Segurança da Informação, devendo reportar-se a eles todo e qualquer usuário e/ou setor para tratar de assuntos pertinentes à segurança da informação dos quais aborda tal instrumento.

2.10 VIGÊNCIA E VALIDADE

A Política Interna de Segurança da Informação passar a vigorar a partir da data a ser estipulada, sendo válida por tempo indeterminado e incidindo sobre todos os colaboradores da empresa, segundo declaração de comprometimento da Direito e Presidência.

2.11 NORMA NBR ISO/IEC 27002:2013 E OS CONTROLES UTILIZADOS NA PSI

A norma NBR ISO/IEC 27002:2013 pode ser considerada como um código de boas práticas a ser implementado e aplicado na organização para a segurança da informação. Esta norma é composta por um conjunto de controles que tem como objetivo a proteção da informação. Para cada um desses são definidas diretrizes que indicam como deve ser implantado o respectivo controle.

Cabe salientar que a escolha dos controles estão diretamente relacionados às decisões da empresa, sopesando os critérios para aceitação de riscos, opções para o seu tratamento e gestão de risco. Ou seja, eles podem não ser totalmente adequados em todas as situações a depender dos requisitos de controle específicos da organização em função de seu estágio de maturidade, grau de informatização, área de atuação, cultura organizacional, entre outros aspectos.

Tabela de controles implementados na PSI

Controle de acesso	**x**
Classificação e tratamento da informação	**x**
Segurança física e do ambiente	**x**
Tópicos orientados aos usuários finais	**x**
Dispositivos móveis e trabalho remoto	**x**
Restrições sobre o uso e instalação de software	**x**
Backup	**x**
Transferência da informação	**x**
Proteção contra códigos maliciosos	**x**
Gerenciamento de vulnerabilidades técnicas	**x**

Controles criptográficos	Não necessita ser empregado, pois as comunicações realizadas dentro dos sistemas na empresa, utilizam criptografia nativamente.
Segurança nas comunicações	**x**
Proteção e privacidade da informação de identificação pessoal	**x**
Relacionamento na cadeia de suprimento	Não necessita ser inserido na PSI, pois as cadeias de suprimentos seguem o rigor dos padrões de qualidade da ISO 9000.

3 CONCLUSÃO

No cenário atual, a área de TI obteve um grande crescimento no mercado, alcançando lugar de destaque e desempenhando papel decisivo nas diversas organizações. Destarte, encontrando-se o mundo movido pela informação, esta deve ser assegurada da melhor forma possível de modo que a organização possa criar suas estratégias e prestar os serviços com a mais alta qualidade, gerando redução de custos, melhorando a eficiência e qualidade dos serviços, por meio da padronização e gerenciamento de cada processo.

Para que os pontos acima citados possam ser seguidos e alcançados pelas empresas, é necessário a implantação da PSI, já que esta mostra-se como a solução mais adequada para o estabelecimento de um conjunto de normas e diretrizes que regulam a utilização dos sistemas nas instituições.

É, pois, de suma importância que as instituições aliem a PSI ao contrato de trabalho dos colaboradores, visto que todo processo de segurança se inicia na contratação. Sendo importante salientar que os colaboradores devem estar cientes da observação das informações.

Dessa forma, a PSI demonstrando seus reais benefícios, deve ser adotada pelas instituições e estabelecida em conjunto entre a área de TI, responsável por criá-la, a gerência e os demais colaboradores.

ABSTRACT

In the face of great competition and mobilization in the business world, it is essential to the use of effective processes and practices for the development of services. Companies then need to win a major challenge, which is the standardization to achieve excellence. For these reasons, the objective of this work is the creation and the implementation of Security Policy Information (PSI) in SUCOSUL, demonstrating that the alignment between the business area and organizational technology is an important management tool. Clarifications about the topic discussed will be carried out through field research conducted in the organizational environment to be implemented the Information Security Policy and literature of exploratory, descriptive and explanatory, which will be used to print books, papers and materials available on the Internet, for discussion, interpretation and development of the established theme. Thus, they will be shown the main activities of the industry IT industry since its inception to the procedures performed in their day to day to ensure the safety of organizational resources. Also the difficulties will be shown, requirements, tools and procedures that are followed in time to deploy a PSI, which will provide strategic facilities for the development of business, such as competitive advantage, cost reduction and standardization that will enable future growth of industry.

Keywords: Development of Industry; Management Environment; Implantation; Network infrastructure; Information security; Security Policy Information.

REFERÊNCIAS

ABNT, **NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

BRASIL. **Consolidação das Leis do Trabalho**. Decreto-lei n° 5.452, de 1° de maio de 1943.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012.

BRASIL. Lei n° 9.610, de 19 de fevereiro de 1998.

BRASIL. Lei n° 9.609, de 19 de fevereiro de 1998.

BRASIL. Lei n° 9.279, de 14 de maio de 1996.

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação - Princípios e Controles de Ameaças.** Série Eixos. Editora Érica, 2014.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação: Guia Prático para Elaboração e Implementação.** 2ª ed. Rio de Janeiro: Editora Ciência Moderna, 2008.